Redacted Version of
Jonathan Hochman 6.7.2022
Rebuttal Report and all Appendices
(Plaintiffs)

[Document sought to be sealed]

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, WILLIAM BYATT, JEREMY DAVIS, CHRISTOPHER CASTILLO, and MONIQUE TRUJILLO, individually and on behalf of all similarly situated,	§	
Plaintiffs,	§	**Case No. 4:20-cv-03664-YGR-SVK**
v.	§	
GOOGLE LLC,	§	
Defendant.	§	

REBUTTAL TO REPORT OF GEORGIOS ZERVAS AND SUPPLEMENTAL REPORT OF JONATHAN E. HOCHMAN

June 7, 2022

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY OF OPINIONS

1. Pursuant to the Court's Standing Order, this section includes an executive summary of each opinion to be proffered.

2. Opinion 1: Professor Zervas opines that "[b]ecause cookie values associated with Private Browsing Sessions are not shared with other browsing sessions, this information cannot be used to link the Private Browsing Mode activity to a user or her device after that Private Browsing Session is closed" (Zervas Report ¶ 6, Opinion 1). As described in Sections V.A and V.D below, it is my opinion that private browsing data collected and stored by Google can be linked with users' Google accounts and other personally identifiable information. Regardless, the private browsing and non-private browsing data for the class members are collected by the same Google services for the same general pool of data. Professor Zervas errs by failing to even consider whether the myriad of data collected by Google from users' private browsing sessions and stored within Google logs can be used identify users and their devices. Such data includes IP address and user agent information, cookies, user identifiers associated with users' accounts on non-Google websites, browsing history, and UMA data. In fact, it appears as if Professor Zervas did not even review the data produced by Google in this case through the Special Master process. I have reviewed this data, and it supports my opinions that Google within its logs reliably identifies traffic as Incognito and that private browsing data stored within Google's logs is linkable to users and their devices. Professor Zervas also ignores numerous internal Google documents that undermine his opinion.

3. Opinion 2: Professor Zervas opines that "Private Browsing Modes on the major browsers provide similar functionality, with some differences in implementation between browsers" (Zervas Report ¶ 3, Opinion 1). As described in Section V.B below, it is my opinion that Professor Zervas's

assertion is incomplete. He ignores key facts, including that Google, unlike other major browser providers, is also a major analytics and advertising service provider—meaning that Google benefits from private browsing information in ways that do not apply to other browser providers.

4. Opinion 3: Professor Zervas opines that private browsing modes "prevent browsing history from being saved on the device" (Zervas Report ¶ 5, Opinion 1). As described in Section V.C below, Professor Zervas's analysis is unreliable and incomplete. He ignores documents produced by Google that undermine his assertion. Moreover, he fails to even address, much less grapple with Google's server-side storage of private browsing information.

5. Opinion 4: Professor Zervas opines that "browsers (including Chrome) have numerous *other* settings and available features that prevent the transmission of certain categories of At-Issue Data" (Zervas Report ¶ 9, Opinion 2). As described in Section V.E, it is my opinion that none of these "settings and available features" serve as an adequate substitute to what Google promised to deliver, namely, a private browsing experience where Google would not be able to collect users' browsing information. These settings are often hidden and unusable, fail to prevent Google's collection of private browsing information, and Google sometimes discourages users from employing them within a private browsing session. And to the extent Google believes these settings and features are important for privacy, Google could have easily implemented them into Chrome Incognito and/or Google tracking beacons.

6. Opinion 5: As described in Section V.E., it is my opinion that had Google preserved its records of private browsing data, Google could use those records to verify whether it collected a user's private browsing information notwithstanding that user's choice to enable any of the foregoing settings or features within a private browsing mode (assuming such a user exists).

7. Opinion 6: Professor Zervas opines that "the Private Browsing modes work as described in public documentation" (Zervas Report ¶ 5, Opinion 1). I disagree. As described in Section V.F, it is my opinion that Google's Chrome Incognito mode functioned in ways that differed from how Google represented it would function. Professor Zervas entirely ignores numerous internal Google documents that undermine his opinion and support mine, including documents where Google employees recognize that users are suffering from "common misconceptions about private mode." He also fails to proffer any support that users understand the promise of private browsing as limited to what is saved on a user's device.

II. STATEMENT OF LIMITATIONS REGARDING THIS REPORT

8. I prepared this report for purposes of this case only. It may not be used for any other purpose. This report contains and refers to information designated as "CONFIDENTIAL" and "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by both parties under a Stipulated Protective Order.

III. ENGAGEMENT

9. Counsel for the Plaintiffs in this action ("Counsel") retained me to develop and render opinions concerning the technology and practices at issue in this litigation with respect to several products developed and distributed by defendant Google, LLC ("Google"). The Google Products include Chrome Incognito and Google tracking code (e.g., Google Analytics and conversion tracking code) and Google advertising code (e.g., Google Ad Manager and Google AdSense advertising code). I submitted my opening expert report on April 15, 2022. My April 15 report contained a section outlining my expertise, and my CV was included as Exhibit A to that report.

10. On the same day, Google's expert, Professor Georgios Zervas, submitted a report (the "Zervas Report") where he provided opinions related to private browser functions and settings.

Counsel asked me to review and provide opinions regarding Professor Zervas's report. I have reviewed the Zervas Report and the materials appended to it.

11. Google has also made additional data productions through the Special Master process since I submitted my opening report. I provide an analysis of those additional data productions in this report as a supplement to my opening report and in connection with my response to the Zervas Report.

12. Those additional Google productions are deficient in several aspects as I describe in this report. Should Google produce additional data shortly before or any time after I submit this report, I reserve my right to further supplement my report.

13. As before, I am charging an hourly rate of $800/hour and my associate, Julie Ann Burns, is charging an hourly rate of $200/hour. Our compensation does not depend upon the outcome of the case. In the event of any recovery in this case, I understand that Ms. Burns and I will be excluded from any disbursement of funds.

IV. PREPARATION

14. As discussed in my opening report, I spent hundreds of hours reviewing materials produced in this case, including documents Google produced as well as deposition transcripts and written discovery responses. I also reviewed extensive data from Google's logs produced through the Special Master process.

15. In preparing this report, I worked with the consultants identified in my opening report, including to analyze additional data that Google produced through the Special Master process after my opening report was submitted on April 15, 2022. This included production of Google UMA, Analytics, and ads data through May 20, 2022. I also directed and supervised consultants in analyzing visits to several popular websites, including the top websites identified by Google in its Supplemental Response to Interrogatory No. 5.

16. My opinions in this report are informed by the voluminous documents and log data I reviewed as well as by the extensive tests conducted by my consulting team at my direction and under my supervision.

V. OPINIONS

A. Contrary to Professor Zervas's stated opinions, private browsing data collected and stored by Google can readily be linked with users' Google accounts and other personally identifying information.

17. While Professor Zervas asserts certain opinions with respect to linking private browsing cookies to a user or to regular mode browsing data,[1] he fails to discuss or analyze cookie values and other fingerprinting information collected and stored by Google in Google logs and data sources during and after each private browsing session. Professor Zervas also fails to discuss or analyze Google's logging of private browsing information when a user is not signed into a Google account but is signed into non-Google websites. Without analyzing Google's data logs and data sources and the information contained within those Google logs and data sources, and without a review of internal Google documentation discussing this issue of data identifiability and linkability, Professor Zervas's opinion regarding the inability to link cookie values to the "user or her device" after a private browsing session closes is unsupported and fails to engage with the relevant issues.

[1] *See e.g.*, Zervas Expert Report: "private browsing modes [] ensure that cookie values generated during the Private Browsing Session cannot be used to provide a link to the user or her device after the session is closed" ¶ 2, "the cookie values generated during the Private Browsing Session cannot be used to provide a link to the user or her device after that session is closed, unless the user explicitly enables a website to make this association by signing into the website during the Private Browsing Session, or enables Google to do so by signing into their Google account during the Private Browsing Session" ¶ 4, "[b]ecause cookie values associated with Private Browsing Sessions are not shared with other browsing sessions, this information cannot be used to link the Private Browsing Mode activity to a user or her device after that Private Browsing Session is closed" ¶ 6 and "cookie values generated during the Private Browsing Sessions cannot be used to provide a link to the user's browsing activity in Regular Mode" ¶ 80.

18. Contrary to Professor Zervas's portrayal of private browsing data as "orphaned islands of data" (Zervas Report ¶ 83), I showed in my April 15th report that there are many ways to link these data to one another. I explained and demonstrated how "information tied to a user's Google account could be linked to the same individual's private browsing information stored within Google logs and data sources" (Opening Report Opinion 18; see also Section VIII.F ("Throughout the class period, Google collected and stored private browsing information in ways that can be joined to other Google user information")). Through concrete examples using data collected by Google and stored in Google logs and data sources, I demonstrated how IP address and user agent as well as user identifiers for non-Google websites can be used to link private browsing information collected by Google and stored in Google logs and data sources to a user and to regular mode data (see Section VIII.F of my opening report). I also showed how cookie values stored in these Google logs and data sources provide an indication of data generated from the same private browsing session on the same device. I also discussed other information stored in Google logs and data sources such as language, URLs visited, timestamps, and other identifiers (such as [redacted]), among other information, that further identify a user or a user's device.

19. I also cited extensive internal Google documentation and deposition testimony supporting my findings, which Professor Zervas has ignored. For example, ¶ 235 of my opening report cites several internal Google documents that state "Currently we are logging all user activities in incognito mode server-side, and that is more or less linkable to users signed-in data" (GOOG-BRWN-00184875), "we already consider it possible for Google to join regular and Incognito sessions" (GOOG-CABR-00489377 at -384), and "IP can be used to join the authenticated and incognito sessions" (GOOG-BRWN-00157001); *see also* McClelland Tr. 212:13-212:24 ("Q. Do

you still agree with the statement, it's possible for Google to join regular and Incognito sessions? . . . A. As far as I know, assuming nothing has changed, then, yes, it should still be possible.").

20. Other internal Google documents ignored by Professor Zervas also support my findings. In February 2020, a Google employee admitted to others that "we would never sa[y] that Google doesn't know who you are while you're Incognito" (GOOG-CABR-04780837.R at -840.R.) [redacted] As I noted in my opening report, Google employees also internally recognize the implication for joinability of collecting IP addresses, admitting that: "When Incognito is on . . . Google . . . save[s] personal data? [and] save[s] IP addresses or other unique IDs" before noting that Google's collection of this information contradicts that the "intention is to be private" (GOOG-CABR-05148261 at -273).

21. Academic studies also undermine Professor Zervas's opinion. As just one example, a 2019 study concluded that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes."[2] It appears that Professor Zervas did not contend with such studies.

22. Professor Zervas also ignores how, as I discussed in Sections VIII.F and VIII.H of my opening report, Google actively tracks Incognito usage and how the detected Incognito traffic can be linked to a user's Google account. For example, I showed in Appendix I of my opening report that consultant Dr. Dai's Incognito data associated with Biscotti ID [redacted] is accurately identified by Google as Incognito traffic, with Google's "maybe_chrome_incognito" field set as "TRUE" in Google's display ads logs for that data. In ¶ 234 of my opening report, I

[2] Luc Rocher, Julien M. Jendrickx and Yves-Alexandre de Montjoye, *Estimating the success of re-identifications in incomplete datasets using generative models*"
https://www.nature.com/articles/s41467-019-10933-3 (July 23, 2019).

described how the IP address and user agent in Google logs and data sources associated with Biscotti ID [redacted] also appear in Dr. Dai's signed-in GAIA logs associated with her Google account GAIA ID. This links the Biscotti ID, which is embedded by Google in Biscotti cookies, to Dr. Dai and her device, including the Incognito browsing data.

23. Since I submitted my opening expert report on April 15, 2022, Google has produced additional data through the Special Master process. On May 18, 2022, Google produced search results using IPv6 address and user agent string combinations as input search parameters as a part of the Third Iterative Search of the Special Master process. This Google production further demonstrates that IP address and user agent can be used to locate a particular user's browsing activities in Google's logs, including for data marked by Google as Incognito data. For example, from Plaintiff Chasom Brown's IPv6 address and user agent[3], Google located a Biscotti ID [redacted] in Google's [redacted] generated in Chrome regular mode browsing.[4] Within Google ad query logs associated with this same Biscotti ID, Google located a PPID-mapped-Biscotti [redacted] associated with Mr. Brown's signed-in PPID (Publisher Provided ID) on vogue.com.[5] As I discussed in my opening report, PPID uniquely identifies a user logged into a non-Google website. Since this PPID is the same regardless of

[3] I understand from Counsel that Google agreed to search with IPv6 and user agent, without disputing that this combination of identifying information uniquely identifies a Plaintiff's device. However, I also understand from Counsel that Google refused to run a search based on a combination of IPv4 address and user agent. By refusing to run this search, Google precluded Plaintiffs from conducting an analysis of that data. As I discussed in my opening report and in this report, in addition to IP address and user agent, Google stores other fingerprinting information in its logs.

[4] See "2022-05-18 Brown v. Google - Google Letter re Final Searches.pdf". The associated output files from the [redacted] search are located in "2022-05-18 Brown v. Google – partnerlog – AEO" as represented by Google in "2022-05-20 Brown v. Google – Search Script Tracker.xlsx" for Third Iterative Search – Search II, Step 1. I have shown in Appendix I of my opening report that Biscotti ID [redacted] is associated with regular mode browsing.

[5] Google represented in "2022-05-18 Brown v. Google - Google Letter re Final Searches.pdf" that the Biscotti ID [redacted] was used to search [redacted] and [redacted] logs and that the file "2022-05-18 Brown v. Google - Decrypted Biscottis from Ad Queries - AEO.pdf" contains decrypted IDs from the [redacted] and [redacted] Three unique decrypted IDs are found in this document: [redacted]

whether a sign-in on vogue.com occurred in regular mode or in Incognito mode, the produced Google ads log data associated with this PPID-mapped-Biscotti [redacted] contain Incognito events with many such event entries marked by Google with "maybe_chrome_incognito" = "true".[6]

24. On May 2, 2022, Google produced 105 decrypted Biscotti and PPID-mapped-Biscotti IDs from preserved GAIA logs for the named Plaintiffs.[7] This Google production further demonstrates that Google's GAIA logs can be used to locate a particular user's PPID-mapped-Biscotti, which in turn, can be used to locate a user's signed-out private browsing data in Google's logs. As I discussed in my opening report, encrypted Biscotti IDs are stored by Google in GAIA logs. Google's May 2nd production further shows that PPID-mapped-Biscottis are also present in GAIA logs. As I show in Appendix A of this report, Biscottis and PPID-mapped-Biscottis not associated with previously submitted search values have been located in the preserved GAIA logs. A search in ads logs using the decrypted Biscotti and PPID-mapped-Biscotti IDs from the preserved GAIA logs located Plaintiffs' data on non-Google websites while not signed into Google, including those marked by Google as Incognito traffic using "maybe_chrome_incognito." Significantly, PPID-mapped-Biscotti IDs link a user's signed-in GAIA data to signed-out data. Moreover, PPID-mapped-Biscotti IDs are uniquely associated with a user logged into a non-Google website (in any browser, in private browsing and non-private browsing mode, and whether or not the user is signed into Google), thereby uniquely identifying a user's data, including private browsing data from Chrome, Safari, and Internet Explorer/Edge.

25. Google produced other PPID data after April 15, 2022, which further demonstrates that PPIDs can be used to locate users' data, including Incognito data and data Google collected from

[6] See production "2022-05-18 Brown v. Google – [redacted] Ads – AEO"
[7] See "2022-05-02 Brown v. Google - Decrypted Biscottis from Preserved Data - AEO.pdf".

users browsing in the other private browsing modes (Safari, Edge, and Internet Explorer[8]). The data that Google produced and the searches conducted to generate this data related to Third Iterative Search – Search III are summarized in Appendix B (in the "Search III prod analysis" tab, columns A to Q).[9] Appendix B also shows how the data produced by Google was incomplete. Despite the deficiencies in Google's production, I conducted an analysis of produced events from April 30 to May 20, 2022 containing PPID-mapped-Biscottis and those events that were located using PPID-mapped-Biscottis. The results are summarized in Appendix C. Column G of the "PPID Analysis" tab includes many PPID-mapped-Biscottis identified as being used in both regular mode and Incognito mode, thereby creating a linkage between regular mode and Incognito mode data. For some of the PPIDs, I show the GAIA IDs in Google's [redacted] logs that are found through a PPID search. This further demonstrates that the linkage between GAIA and PPID goes both ways.

26. On May 7, 2022, Google produced search results based on an Analytics UID (User ID) search as a part of the Third Iterative Search – Search IV of the Special Master process.[10] This Google production demonstrates that Analytics UID can also be used to locate a particular user's browsing activities, including traffic identified by Google as Incognito. As I discussed in my opening report, Analytics UID uniquely identifies a user logged into a non-Google website. Like

[8] *See e.g.*, productions in "2022-05-20 Brown v. Google - [redacted] Set 1" and Appendix C.

[9] Part of Google's PPID data production was conducted as a part of the Third Iterative Search, Search III. In this particular search, Plaintiffs asked Google to produce data using IDs found in [redacted] logs based on searching these logs with submitted PPIDs, IDs in preserved GAIA logs, and IDs in [redacted] based on searching this log with submitted IP address and user agent pairs. As I explain in Appendix B of this report, Google failed to include numerous IDs found in [redacted] for this search, resulting in an incomplete production. What Google should have produced is shown in Appendix B (in the "Search III prod analysis" tab, columns S to W).

[10] Google represented in "2022-05-20 Brown v. Google – Search Script Tracker.xlsx" for Third Iterative Search – Search IV, Step 1 the output Analytics files based on a search of submitted Analytics User IDs (UIDs) are found in "2022-04-30 Brown v. Google - Analytics – AEO". These output files contain Analytics UIDs as well as Biscotti IDs.

PPID, Analytics UID identifies a user browsing in any browser, in private browsing and non-private browsing mode, and whether or not the user is signed into Google. Search IV of the Third Iterative Search searched Analytics logs with Analytics UIDs and located Biscotti IDs within Analytics logs associated with the Plaintiffs' and Dr. Dai's devices, including Biscotti IDs that have never been submitted as search parameters in the Special Master process (see Appendix D).[11] As with PPIDs, in Appendix D, column G of the "UID Analysis" tab, I include many Analytics UIDs identified as being used in both regular mode and Incognito mode, thereby creating a linkage between regular mode and Incognito mode data.

27. After April 15, 2022, Google also produced additional event records that include Google's Incognito detection fields. Both for the purpose of responding to the Zervas Report and to supplement the analysis in my original report, I analyzed the data produced by Google where the events were marked by Google with "is_chrome_incognito" and "maybe_chrome_incognito" as "TRUE" or "FALSE."

28. With Google having now produced over [redacted] event entries with one or both of those two Google Incognito-detection fields marked as TRUE or FALSE, and having tracked at the outset the mode associated with those events, I have determined that there is a 99.89% accuracy on an

[11] Six previously submitted Biscotti IDs and seven Biscotti IDs that have not been submitted for search in the Special Master process were located through a search with Analytics UIDs (See Appendix D, "Biscottis Found by UID" tab and "UID Analysis" tab). The search also located ten additional Biscotti IDs that are not associated with submitted UIDs and web properties (See Appendix D, "Unknown Biscottis" tab; none of the events associated with these Biscottis match the submitted website properties). On May 18th, 2022, Google produced the Analytics UID search script (2022-05-18 Brown v. Google – Analytics Scripts – AEO.pdf), which revealed that Google did not limit the UID search results to UIDs associated with the submitted websites; therefore, finding additional Biscotti IDs is not surprising. Some of these Biscotti IDs may not be associated with Plaintiff and Dr. Dai's data. While UIDs are unique to a particular website property, there may be collisions across different website properties. Had Google conducted the search properly limiting UID events to only those associated with submitted website properties, these extraneous Biscotti IDs ("Unknown Biscottis") would not have been found by a UID search as I have shown in Appendix D.

event-by-event basis for those two Incognito detection fields, and also a 100% accuracy rate if you consider these records by ID instead of by event. [12]

29. As I discussed in my opening report, evaluating these Incognito detection fields across data sets for specific user identifiers achieves greater accuracy and can eliminate what Google's employees have referred to "edge cases." With such analysis, based on the data stored by Google and produced by Google as part of the Special Master process, I have determined that Incognito detection accuracy for "is_chrome_incognito" and "maybe_chrome_incognito" using the data collected and stored by Google associated with different Zwieback and Biscotti IDs to be 100% for the produced dataset. This analysis is shown in Appendix E of this report.

30. After April 15, 2022, Google also produced data containing the x-client-data header field. To respond to Professor Zervas's Report and to supplement my opening report, I analyzed events within the produced datasets that contain that x-client-data header field (from [redacted] [13]). Following the same analytical steps I described in my opening report, I determined that Google's x-client-data-based Incognito detection accuracy is 100% for the produced dataset when evaluated across each user's dataset. Even when looking at the data on an event-by-event basis, the accuracy in terms of identifying regular mode and Incognito mode browsing events based on the absence of the x-client-

[12] Of the over[redacted] entries, there were[redacted] entries where the maybe_chrome_incognito field was set to "true" where the browsing was in Regular mode. Having evaluated those events, I have determined the error was not due to any inaccuracy within the maybe_chrome_incognito algorithm. For those 15 events, the Chrome browser was not sending x-client-data in an edge case scenario associated with Dr. Dai's test device over a brief period, evidently because of Chrome freezing (unresponsive) and device reboot. This is consistent with Google engineer Chris Liao's testimony that there may be some edge cases. *See* Apr. 21, 2022 Hearing Tr. at 169:1-8 ("There are edge cases, there are cases in Chrome, and also non-Chrome browsers where we wouldn't be able to serve this header that is outside of Incognito mode.").

[13] In Google's response and supplemental response to Interrogatory No. 34, Google represented that its engineers have considered [redacted] in the 2020 Incognito analysis: [redacted]. In [redacted]", Google represented that the [redacted] is no longer collecting data as of March 11, 2020. From the produced data, I have seen no evidence of HTTPHeader and x-client-data being logged in the [redacted] log.

data header in addition to user agent (indicating Chrome on non-iOS devices) is [redacted] across over [redacted] produced Chrome regular mode and Incognito mode event entries. The event-level inaccuracies are due to [redacted] event entries out of the previous total in Chrome regular mode that do not contain x-client-data. This analysis is shown in Appendix F of this report.

31. The data produced by Google also demonstrates that Biscotti and Zwieback cookies (from either regular mode or Incognito mode) can be linked to a user and a user's device. Zwieback data (associated with Google searches) can also be linked to data Google collects when users visit non-Google websites, which I have shown using concrete examples in my opening report. Furthermore, this linkage can be demonstrated with data produced after the submission of my opening report.

32. On April 22, 2022, Google produced [redacted] event entries within a Google search location log called [redacted] [14] This Google log has contained an "is_chrome_incognito" field since at least 2017, as I explained in my opening report. Google's proto comment for the "is_chrome_incognito" field states that the field "Represents if an entry comes from a Chrome web browser in the incognito mode." [15]

33. I have included a copy of those 11 Google log entries in Appendix G, in the [redacted] tab. As can be seen in Appendix G, in addition to the "is_chrome_incognito" field, this log contains timestamp, Zwieback cookie id, location information of the user (longitude, latitude and other location and location context information amounting to an average of more than 30,000 characters per event), Google search queries (such as "eyewear", "kid toys" and "tesla cars"), type of device, operating system, type of browser, IP address, user agent, display language, and more. These Google log entries also contain a field called "fingerprint."

[14] 2022-04-22 Brown v. Google - [redacted] - AEO
[15] 2022-04-01 Brown v. Google - Google Letter.pdf

34. In the [redacted] tab of Appendix G, I show in columns A to E a reproduction of the IP address, user agent, Zwieback cookie ID, search query term, and "is_chrome_incognito" fields from the [redacted] data produced by Google. The "is_chrome_incognito" includes either TRUE or FALSE, with those values set by Google. In column F, I show the actual browsing mode associated with each Zwieback cookie. Column G shows that the values set by Google with the "is_chrome_incognito" field are 100% accurate for this dataset.

35. I asked consultants Mr. Thompson and Dr. Dai to provide supporting HTTP information extracted from data captures from Plaintiffs' and Dr. Dai's devices. These data captures were provided in Exhibit F of my opening report.[16] Supporting information for each Zwieback cookie is shown in the "[redacted] tab of Appendix G, columns H to J. As can be seen, Chrome traffic in regular mode contains x-client-data in column J while Chrome traffic in Incognito mode does not.

36. With the fingerprinting information stored by Google in these Google logs (e.g., search query, IP address, user agent string, geolocation, timestamp), one can readily link those entries (containing a user's private browsing information from visits to non-Google websites while not signed into any Google account) to the user or the user's device. This is consistent with the recognition by numerous Google employees that such linking is possible, ignored by Professor Zervas. This linking is significant in part because when a user opens a new Incognito window, the first action is usually a Google search in the URL box. For example, a search of "eyewear" will result in ads and search results related to eyewear. Clicking on either an ad or a search result will take the user to a non-Google website related to eyewear.

[16] An additional data capture file cited in Appendix E is included in Exhibit B of the current report.

37. As an example, I will discuss three Incognito events in the produced [redacted] that overlap in time with events in search and display ads logs and show that these events can be joined with a user's device and/or the user's GAIA ID.

38. The produced [redacted] log events included in Appendix G of this report show two entries on April 14, 2022, containing search queries [redacted] and [redacted] Both events have "is_chrome_incognito" marked as "TRUE" (correctly indicating Incognito mode browsing), Zwieback ID [redacted] IP address [redacted] and user agent [redacted] These two events in Google's logs were generated by browsing with Dr. Dai's device. The produced [redacted] log data also shows one entry on April 13, 2022, containing search query [redacted] This event has "is_chrome_incognito" marked as "TRUE" (correctly indicating Incognito mode browsing), Zwieback ID [redacted] IP address [redacted] and user agent [redacted] This event in Google's logs was generated by browsing with Plaintiff Chasom Brown's device.

39. **Example 1** associated with search query [redacted] After searching [redacted] in Incognito mode, Google search ads associated with the same Zwieback ID, IP address, user agent and search query appear in the [redacted] log at the same time. A related event in [redacted] with the same time, Zwieback ID, search query, IP address and user agent shows "maybe_chrome_incognito" to be "TRUE." A subsequent search ad click appears in the [redacted] a few seconds later and is associated with the same Zwieback ID, IP address, user agent and ad URL. This search ad click is first transmitted to Google, where Google appends a click ID (gclid) identifying the ad click (and search query) to the landing page URL and redirects

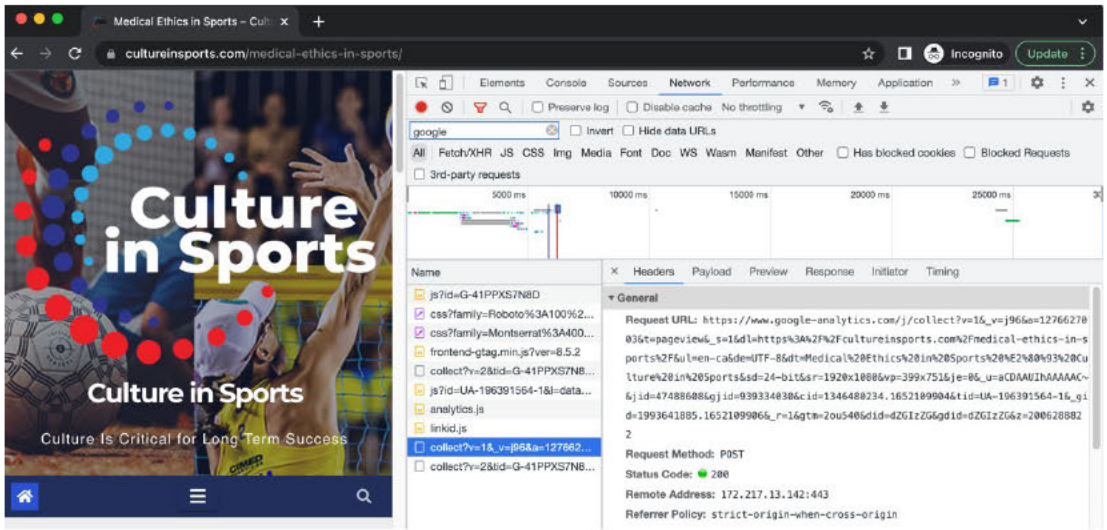
the user to the non-Google website. The redirect URL is [redacted] Once the user is on this non-Google website, in Incognito mode, Google intercepts private communications with at least Google Analytics tracking beacons on this website, which results in Google collecting and storing private browsing information from the private communication between the user and that non-Google website.

40. This series of browsing activities is listed in the table below along with a screenshot showing Google Analytics tracking beacons sending intercepted data to Google in Incognito mode when visiting "https://cultureinsports.com/medical-ethics-in-sports." Google stores the private browsing activities of the user on this non-Google website in at least Google's Analytics logs. For example, from the Second Iterative Search, Google has produced Analytics data stored in urchin:analytics_collection and web_property_hits among other Analytics logs. [17]

Log [18]	Type	Event Time	IP/User agent	Event
[redacted]	Oolong	1649978902661754000 (Thu Apr 14 2022 23:28:22 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649978902839924 (Thu Apr 14 2022 23:28:22 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649978902839924 (Thu Apr 14 2022 23:28:22 GMT+0000)	[redacted]	[redacted]

[17] See "2022-03-25 Brown v. Google – Analytics [redacted] data – AEO" and "2022-03-15 web_property_hits"
[18] The [redacted] log was produced in "2022-04-22 Brown v. Google - [redacted] – AEO" and the ads logs were produced in "2022-04-30 Brown v. Google - [redacted] Ads – AEO".

[redacted]	Search ads	164997891137 3234 (Thu Apr 14 2022 23:28:31 GMT+0000)	[redacted]	[redacted]



41. **Example 2** associated with search query [redacted] Similarly, after searching [redacted] Google search ads associated with the same Zwieback ID, IP address, user agent and search query

appear in Google's [redacted] at the same time. The entry in Google's [redacted] log further confirms these log entries as Incognito traffic with maybe_chrome_incognito set to "TRUE" along with other identifying information. A subsequent search ad click appears in Google's [redacted] a few seconds later and is associated with the same Zwieback ID, IP address, user agent and ad URL. This Google search ad click is first transmitted to Google, where Google appends a click ID (gclid) identifying the ad click (and search query) to the landing page URL and redirects the user to the non-Google website. The redirect URL is [redacted] Once the user is on this non-Google website, Google intercepts private communications with at least Google Analytics and conversion tracking beacons as shown in the screenshot below. Subsequent Incognito browsing activities on non-Google websites with Google tracking beacons appear in Google's display ads logs, including [redacted] and [redacted]. In addition, [redacted] associated with the same Biscotti ID [redacted] with maybe_chrome_incognito" equal to "TRUE" contains a PPID-mapped-Biscotti [redacted] along with other identifying information. This hex value is equal to [redacted].[19] and corresponds to Dr. Dai's signed-in PPID on marca.com[20], thus further identifying these Incognito events as her browsing activities. Additionally, from Google's Analytics log [redacted]"[21], Dr

[19] Hex to decimal value conversion can be done here https://www.rapidtables.com/convert/number/decimal-to-hex html

[20] Google provided PPID to PPID-mapped-Biscotti mapping in the Second Iterative Search "2022-03-04 Brown Second Iterative Searches - PPID.xlsx"

[21] From "2022-04-30 Brown v. Google - Analytics – AEO"

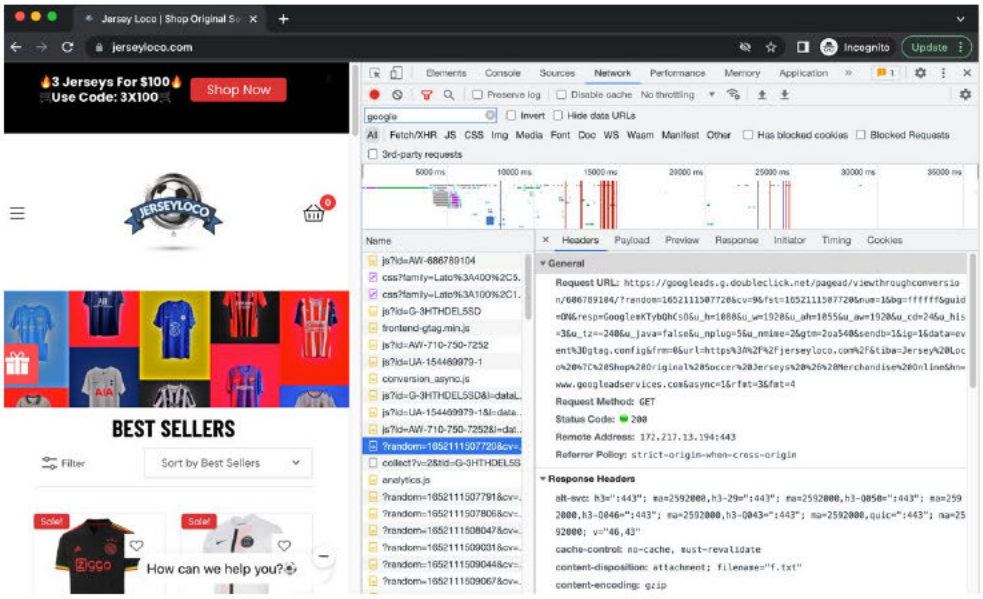
Dai's Biscotti ID is associated with her Analytics user ID [redacted] on marca.com, which also further identifies these Incognito events as her browsing activities. This series of correlated browsing activities is listed in the table below.

Log[22]	Type	Event Time	IP/User agent	Event
[redacted]		1649978942655483000 (Thu Apr 14 2022 23:29:02 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649978942839388 (Thu Apr 14 2022 23:29:02 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649978942839388 (Thu Apr 14 2022 23:29:02 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649978964502212 (Thu Apr 14 2022 23:29:24 GMT+0000)	[redacted]	[redacted]

[22] The ads logs are from Third Iterative Search, "2022-04-30 Brown v. Google - [redacted] Ads – AEO"; the Analytics log is from "2022-04-30 Brown v. Google - Analytics – AEO"

[redacted]	Display ads	1649978992264637 (Thu Apr 14 2022 23:29:52 GMT+0000)	[redacted]	[redacted]
[redacted]	Display ads	1649979002210728 (Thu Apr 14 2022 23:30:02 GMT+0000)	[redacted]	[redacted]
[redacted]	Display ads	1649979046460740 (Thu Apr 14 2022 23:30:46 GMT+0000)	[redacted]	[redacted]
[redacted]	Display ads	1649979645968572 (Thu Apr 14 2022 23:40:45 GMT+0000)	[redacted]	[redacted]
[redacted]	Google Analytics	EventID. "time_usec":"1650223743339831"	[redacted]	[redacted]

[redacted]		(Sun Apr 17 2022 19:29:03 GMT+0000)	[redacted]	[redacted]



42. One could form a complete time-series of browsing activities for a user. This time-series would include private browsing activities on the initial Incognito screen (recorded either to google.com as a search event or, if the user types in a complete URL of a website with Google tracking beacons, in Analytics and display ads logs) as well as on YouTube and non-Google websites containing Google tracking beacons like what I have shown here. For example, Google search ad click redirect_url in [redacted] appears in display ad [redacted] thereby making it possible to join search and display information. As an example, the table below contains two events produced by Google in connection with the Second Iterative Search, in 2022-03-14 Brown v. Google – [redacted] – AEO, that shows joining of Zwieback and Biscotti data using

[23] "2022-05-07 Brown v. Google - Decrypted Biscottis - AEO.csv"

time stamp and event URL. The IP address and user agent further confirm these events belong to the same user.

Log[24]	Type	Event Time	IP/User agent	Event
[redacted]	Search Ad log	1641219603975138 (Mon Jan 03 2022 14:20:03 GMT+0000)	[redacted]	[redacted]
[redacted]	Display Ad log	1641219606309649 (Mon Jan 03 2022 14:20:06 GMT+0000)	[redacted]	[redacted]

[24] As I discussed in my opening report, the Zwieback ID and Biscotti ID in this table are associated with Dr. Dai's Incognito mode traffic.

				No x-client-data

43. The signed-out search and display ads logs cited above contain additional identifying information. For example, the following two events in signed-out search and display ads logs both contain similar time, related query and page content, IP address, user agent, country, region, and browser dimension information.

Search Ads Log:	Display Ads Log:
[redacted]	[redacted]

44. Furthermore, information collected and stored by Google from a user's signed-out activities can be linked with the user's GAIA ID. For example, the following GAIA and display

ads logs[25] share not just the same IP address and user agent, but also browser timing, language, and bandwidth, as well as geographical attributes.

[redacted]	**GAIA log:** [redacted]	**GAIA log:** [redacted]	**Signed-out Incognito Display Ads log:** [redacted]
query.query_id.time_usec: "1649977935082954" (Thu Apr 14 2022 23:12:15 GMT+0000)	query.query_id.time_usec: "1649974404913416" (Thu Apr 14 2022 22:13:24 GMT+0000)	query_id.time_usec: "1649978867710154" (Thu Apr 14 2022 23:27:47 GMT+0000)	"query_id.time_usec: 1649979645968572 (Thu Apr 14 2022 23:40:45 GMT+0000)
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[25] From the "2022-04-30 Brown v. Google - [redacted] Ads – AEO" production

45. Not only can signed-out private browsing information collected and stored by Google be linked to a user's GAIA ID, it can also be linked to a user's device UMA ID, which uniquely identifies a Chrome instance on a device and also includes additional information regarding the use of Chrome Incognito mode. For example, the sequence of UMA user actions associated with Dr. Dai's UMA client_2 ID in the table below can be correlated to the above Incognito browsing records stored by Google.[26] UMA data further confirms that a new Incognito window was opened and that the above browsing activities associated with search queries [redacted] and [redacted] as well as subsequent browsing activities on non-Google websites, were generated in Incognito mode. Using UMA, Google also collects and stores a wealth of information about users and their devices, including gender and birth year, IP address, user agent, user location, UMA enabled date, as well as a staggering amount of hardware information (e.g., CPU architecture, system RAM, GPU vendor/device/driver version, screen width and height, screen scale factor, among others).[27] Such information is highly identifying even for two devices sharing a common IP address.

[26] Data from production "2022-04-22 Brown v. Google - UMA – AEO", file "2022-04-14.txt". This document contains coded user actions which the Plaintiffs decoded. The decoded file is included as Exhibit A to this report. UMA user actions and timestamps associated with ads data shown is included in Appendix H, "Apr 14" tab.
[27] GOOG-BRWN-00032906 at -907 explains that UMA stores "system_profile: The system_profile is a proto containing information about the client's browser and system configuration. This has a large set of fields and includes information such as application version, channel, operating system, hardware (such as memory), stability data, plugins installed, field trials (Finch experiments) running, and much more."

User Action Event	time_sec	Date and Time [28]	Ads log and Annotations
NewIncognitoWindow	2177491	2022-04-14 23:27:54	Opened a new Incognito window
NewIncognitoWindow2	2177491	2022-04-14 23:27:54	
ActiveTabChanged	2177491	2022-04-14 23:27:54	
ActiveBrowserChanged	2177491	2022-04-14 23:27:54	
ActiveBrowserChanged	2177491	2022-04-14 23:27:54	
NavEntryCommitted	2177491	2022-04-14 23:27:54	Browsing commences in this new Incognito window
OmniboxInputInProgress	2177503	2022-04-14 23:28:06	User types in the URL box
LoadURL	2177506	2022-04-14 23:28:09	URL is loaded
NavEntryCommitted	2177506	2022-04-14 23:28:09	Page visited
NavEntryCommitted	2177506	2022-04-14 23:28:09	
NavEntryCommitted	2177513	2022-04-14 23:28:16	
NavEntryCommitted	2177513	2022-04-14 23:28:16	
NavEntryCommitted	2177514	2022-04-14 23:28:17	
NavEntryCommitted	2177514	2022-04-14 23:28:17	
OpenFileSystemTemporary	2177516	2022-04-14 23:28:19	
NavEntryCommitted	2177519	2022-04-14 23:28:22	
NavEntryCommitted.SRP	2177519	2022-04-14 23:28:22	Search results page [redacted]
NavEntryCommitted	2177520	2022-04-14 23:28:23	
NavEntryCommitted.SRP	2177520	2022-04-14 23:28:23	
NavEntryCommitted	2177530	2022-04-14 23:28:33	User clicked on a search ad and was redirected to a non-Google website containing at least Google Analytics tracking beacons [redacted]

[28] Google has not explained the method to convert UMA user action event offset timestamps to actual times. Google's response to Plaintiffs' question merely addresses how the event offset timestamps are generated, not how Google computes the absolute times (See 2022-05-18 Brown v. Google - Google Letter to SM and Plaintiffs re Final Searches.pdf). However, this particular UMA record shows that the log creation timestamp is 1649977363 (Thu Apr 14 2022 23:02:43 GMT+0000), and the closing timestamp is 1649979165 (Thu Apr 14 2022 23:32:45 GMT+0000). From the [redacted] log, we know that the time between a search query o[redacted] and a search query o[redacted] is 40 seconds. These correspond to two different NavEntryCommitted.SRP (Search Results Page) events 40 seconds apart. I have mapped these two events to the UMA user actions within the log creation and log closing times. *See* Appendix H.

[29] Ad click time is slightly offset from UMA time which marks page load time after the click.

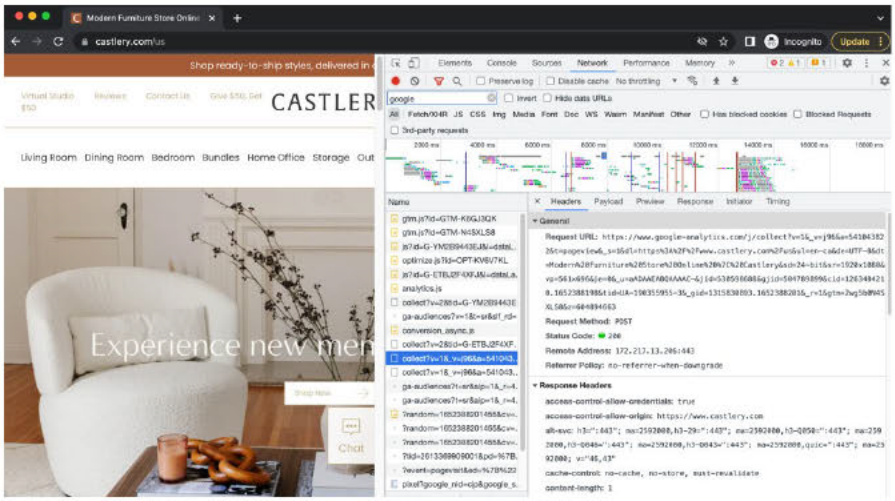
			[redacted]
Back	2177534	2022-04-14 23:28:37	
NavEntryCommitted	2177534	2022-04-14 23:28:37	
NavEntryCommitted.SRP	2177534	2022-04-14 23:28:37	
NavEntryCommitted	2177550	2022-04-14 23:28:53	
OmniboxInputInProgress	2177553	2022-04-14 23:28:56	
OmniboxDestinationURLIsSearchOnDSP	2177559	2022-04-14 23:29:02	
LoadURL	2177559	2022-04-14 23:29:02	
NavEntryCommitted	2177559	2022-04-14 23:29:02	
NavEntryCommitted.SRP	2177559	2022-04-14 23:29:02	Search Results Page [redacted]
NavEntryCommitted	2177560	2022-04-14 23:29:03	
NavEntryCommitted.SRP	2177560	2022-04-14 23:29:03	
NavEntryCommitted	2177564	2022-04-14 23:29:07	
NavEntryCommitted	2177565	2022-04-14 23:29:08	
OpenFileSystemTemporary	2177565	2022-04-14 23:29:08	
Back	2177570	2022-04-14 23:29:13	
NavEntryCommitted	2177571	2022-04-14 23:29:14	
NavEntryCommitted.SRP	2177571	2022-04-14 23:29:14	
Media.Hidden	2177571	2022-04-14 23:29:14	
NavEntryCommitted	2177585	2022-04-14 23:29:28	User clicked on a search ad and was redirected to a non-Google website containing at least Google Analytics and conversion tracking beacons [redacted]

Media.Hidden	2177585	2022-04-14 23:29:28	
OmniboxInputInProgress	2177595	2022-04-14 23:29:38	
LoadURL	2177597	2022-04-14 23:29:40	
NavEntryCommitted	2177598	2022-04-14 23:29:41	
OpenFileSystemTemporary	2177598	2022-04-14 23:29:41	
OpenFileSystemTemporary	2177600	2022-04-14 23:29:43	
NavEntryCommitted	2177608	2022-04-14 23:29:51	[redacted]
OpenFileSystemTemporary	2177608	2022-04-14 23:29:51	
OpenFileSystemTemporary	2177609	2022-04-14 23:29:52	
NavEntryCommitted	2177618	2022-04-14 23:30:01	[redacted]
OpenFileSystemTemporary	2177618	2022-04-14 23:30:01	
OpenFileSystemTemporary	2177619	2022-04-14 23:30:02	
NavEntryCommitted	2177631	2022-04-14 23:30:14	

46. **Example 3** associated with search query "furniture": Similarly, associated with Plaintiff Chasom Brown's Incognito data, after searching "furniture", I was able to trace through the various Google logs to a search ad click activity leading to a non-Google website with Google Analytics and conversion tracking beacons as demonstrated in the screenshot below. Subsequent Incognito browsing activities on non-Google websites with Google tracking beacons appear in Google display ads logs. In addition, [redacted] associated with the same Biscotti ID [redacted] with maybe_chrome_incognito" equal to "TRUE" contains a PPID-

[30] Display ad query event marks ad query time and are slightly offset from the UMA record timestamp which marks page load time.

mapped-Biscotti [redacted] along with other identifying information. This hex value corresponds to Mr. Brown's signed-in PPID on globo.com[31]. This series of correlated browsing activities is listed in the table below. As mentioned earlier, one could form a complete time-series of browsing activities for a user, including activities on google.com, YouTube and non-Google websites containing Google tracking beacons like what I have shown here.

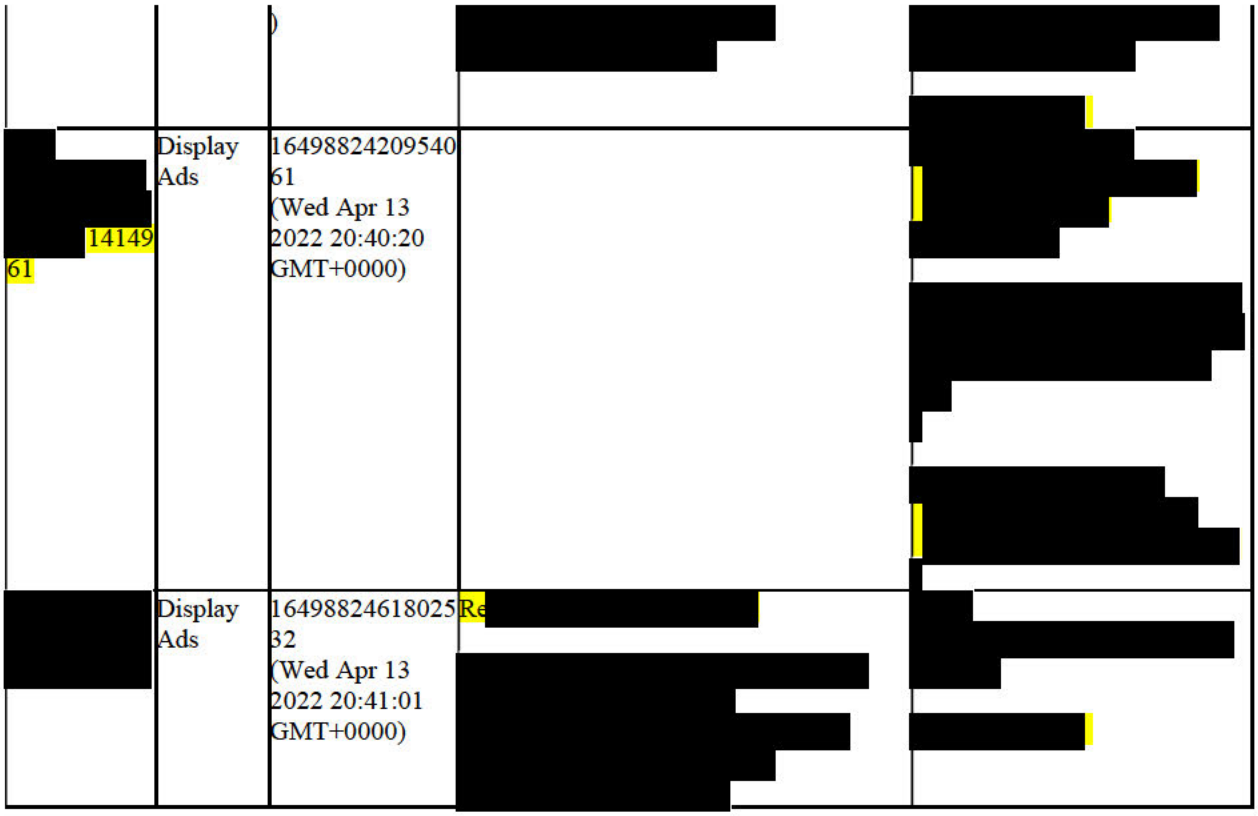


Log[32]	Type	Event Time	IP/User agent	Event
[redacted]	[redacted]	1649881498380199000 (Wed Apr 13 2022 20:24:58 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649881498573998 (Wed Apr 13 2022 20:24:58 GMT+0000)	[redacted]	[redacted]
[redacted]	Search ads	1649881498573998 (Wed Apr 13 2022 20:24:58 GMT+0000)	[redacted]	[redacted]

[31] This PPID-mapped-Biscotti also appears in production "2022-04-30 Brown v. Google - [redacted] Ads – AEO", file [redacted] which contains Mr. Brown's regular mode browsing information.

[32] The ads logs are from Third Iterative Search, "2022-04-30 Brown v. Google - [redacted] Ads – AEO"; the Analytics log is from "2022-04-30 Brown v. Google - Analytics – AEO"

	Search ads	1649881511500631 (Wed Apr 13 2022 20:25:11 GMT+0000)		
	Display Ads	1649882071657422 (Wed Apr 13 2022 20:34:31 GMT+0000)		
	Display Ads	1649882131655575 (Wed Apr 13 2022 20:35:31 GMT+0000)		
	Display Ads	1649882147177258 (Wed Apr 13 2022 20:35:47 GMT+0000		



47. Within the data collected and stored by Google, Mr. Brown's private browsing data can similarly be linked with his UMA events. For example, as I show in Appendix H, "Apr 13" tab, the same IP address and user agent in the table above are also found in UMA data. Furthermore, UMA user actions corresponding to the private browsing information above are shown below. Additional events are shown in Appendix H.

User Action Event	time_sec	Date and Time [33]	Ads log and Annotations
NewIncognitoWindow	6472845	2022-04-13 20:24:20	Opened a new Incognito window
NewIncognitoWindow2	6472845	2022-04-13 20:24:20	
ActiveTabChanged	6472845	2022-04-13 20:24:20	
ActiveBrowserChanged	6472845	2022-04-13 20:24:20	
ActiveBrowserChanged	6472845	2022-04-13 20:24:20	

[33] I show in Appendix G that from the [redacted] log, we know the time between a search query of [redacted] and a search query of [redacted] is 3127 seconds. These search query times correspond to two different NavEntryCommitted.SRP events 3127 seconds apart. I have mapped these two events to the UMA user actions within the log creation and log closing times.

NavEntryCommitted	6472846	2022-04-13 20:24:21	Browsing commences in this new Incognito window
OmniboxInputInProgress	6472866	2022-04-13 20:24:41	User types in the URL box
LoadURL	6472869	2022-04-13 20:24:44	URL is loaded
NavEntryCommitted	6472871	2022-04-13 20:24:46	Page visited
NavEntryCommitted	6472871	2022-04-13 20:24:46	
NavEntryCommitted	6472882	2022-04-13 20:24:57	
NavEntryCommitted.SRP	6472882	2022-04-13 20:24:57	
NavEntryCommitted	6472883	2022-04-13 20:24:58	
NavEntryCommitted.SRP	6472883	2022-04-13 20:24:58	Search results page [redacted]
NavEntryCommitted	6472884	2022-04-13 20:24:59	
NavEntryCommitted.SRP	6472884	2022-04-13 20:24:59	
NavEntryCommitted	6472897	2022-04-13 20:25:12	User clicked on a search ad and was redirected to a non-Google website containing at least Google Analytics and conversion tracking beacons [redacted]
Autofill_ParsedProfileForm	6472901	2022-04-13 20:25:16	
Autofill_ParsedProfileForm	6472905	2022-04-13 20:25:20	
Back	6472910	2022-04-13 20:25:25	

48. The amount of data Google stores from users' browsing activities is staggering. In the table below, I summarize the average number of lines of data Google stores in various logs for a single

event entry, each event entry containing a few kilobytes to a few megabytes of data on average.[34] These averages are taken over the total number of produced event entries for each log.

Log Name	Average Lines per Event Entry	Average Size per Event Entry (Bytes)	Total Number of Event Entries
[redacted]			

49. In Appendix J, I show six sample Incognito event entries stored in six different Google logs, each event entry is the first that appears in the respective log file. These event entries fill over 250 pages at size 5 font.

[34] This data is compiled from data stored in Google ads logs produced between April 30 to May 20, 2022.

50. In Appendix K, I show a small subset of parameters stored in various Google logs (UMA, [redacted] Display ads, Search Ads, signed-in GAIA and Analytics) produced during the Special Master process. These parameters include Incognito detection bits, time stamps, URLs (visited URL or URL of the HTTP request), identifiers, IP address, user agent, browser and device information, geolocation, and other fingerprinting information. The percentage values indicate the percentage of event entries in the produced log files containing the corresponding parameter. A "0%" does not mean that the log does not contain the parameter in general – it means that the parameter does not appear in the produced data for the log either because the parameter does not exist during the produced data period or because Google has omitted certain parameters during production. As can be seen in this table, many fingerprinting information are stored in different types of logs and across signed-in and signed-out ID spaces. For example, I have highlighted Biscotti values and PPID-mapped-Biscotti across different signed-out display ads, analytics and GAIA logs.

51. Given the large volume of detailed fingerprinting information Google collects and stores, the data that Google collects can be readily used to identify users and their devices. The only exception might be if two people, throughout the class period, have identical devices with the same IP address and user agent (same browser version and operating system version), are browsing in Incognito mode at exactly the same time, running exactly the same searches at the same time, and then visiting exactly the same websites at the same time and clicking on the same ads at the same time. This hypothetical scenario of two people having identical devices and the same private browsing activities at the same times across the entire class period is so improbable as to be effectively impossible. Regardless, it is my understanding that Google has not produced any statistics regarding the prevalence of such edge cases, if there even are any.

52. As the productions from the Special Master process demonstrate, and contrary to what Professor Zervas seeks to convey in his report regarding how private browsing mode functions, there are multiple ways to identify a user's private browsing data within the voluminous data that Google collects and stores. One can start from IP address and user agent, GAIA ID, PPID, Analytics UID, "pseudonymous" identifiers (such as Biscotti or Zwieback) or [redacted] and use those to locate other identifiers and log entries containing a user's private browsing information, including log entries with Incognito detection bits marked by Google as "true". The same information can also be used to verify an individual's claim that he or she used Incognito mode to browse a non-Google website while signed out of Google.

53. Professor Zervas's opinion asserting Google's inability to create user profiles in private browsing mode is also unreliable because it contains no discussion of any actual logged data or relevant internal documents.[35] I discussed extensively in Section VIII.E of my opening report how user profiles in [redacted] are generated based on private browsing information. For example, in Section VIII.E.1 of my opening report, I showed concrete examples of user profile information in Google storage based on Plaintiffs' Incognito data, including user profile information keyed to Biscotti IDs and PPID-mapped-Biscotti IDs. I also cited multiple Google internal documents discussing user profiles and their use for ad targeting. For example, in Section VIII.E.2 of my report, I cited Google internal documents stating "Targeted advertising occurs based on data from current Incognito session (tracking) cookies can be placed while Incognito" (GOOG-BRWN-00147873 at -877) and "Users overestimate the protections that Incognito provides and are

[35] See for example, ¶ 6 of Professor Zervas's report where he states: "As a result, these cookie values cannot be used to link the Private Browsing Mode activities to a user or her device after that Private Browsing Session is closed, which would prevent Google from using the cookie values to create a 'cradle-to-grave profile of users,' as Plaintiffs allege."

unaware of the personalization and data collection that occurs when it is on" (GOOG-BRWN-00529122).

54. Professor Zervas's report reflects no review or consideration of any of the actual Plaintiffs' (or other class members') data, nor consideration of the key internal Google documentation cited in my reports. Notably, the data joining exercises I discussed in this section use Plaintiffs' data that Plaintiffs obtained from the same pool of logs collected by the same set of Google services. This means that regardless of "joinability," all of the private browsing and non-private browsing data were generally collected and used by the same Google services.

B. Professor Zervas ignores that Google built functionality designed to track and collect information from all private browsing, for the full class period and across all class members.

55. I have the following responses to Professor Zervas's opinion that "Private Browsing Modes on the major browsers provide similar functionality, with some differences in implementation between browsers" (Zervas Report ¶ 3):

56. First, Professor Zervas ignores the functionality at issue in this lawsuit - which is the *Google* functionality, designed by Google to allow Google to intercept private browsing communications between users and non-Google websites. That Google functionality was the same across the major browsers, across users, and throughout the class period. Professor Zervas notes that "Even in Private Browsing Mode, web browsing necessarily involves transmission of messages from a user's browser—otherwise the webpages would not render. The transmission of those messages must conform to protocols and standards, such as the HTTP protocol, and include information such as IP addresses." ¶ 7. It is true that transmission of messages must occur to render webpages in private browsing mode; however, that transmission is between the user and the non-Google website. Google is not a party to the private communication between the user and non-

Google websites. Nor is Google's interception and subsequent storage and use of that information required by any protocol or standard.

57. Second, Professor Zervas ignores the fact that Google, unlike other major browser providers, provides both a browser and analytics/ads services that are implemented through tracking beacons present on most top websites, as explained in Sections VIII.E and VIII.I of my opening report. While the Chrome browser and other browsers may "discard[] any browsing history or cookies that were stored by the browser during the Private Browsing Session" on users' devices, as Professor Zervas states in ¶ 4 of his report, Google retains such information stored on its server-side. Google then uses private browsing history and cookies it has collected by intercepting private browsing communications, including with non-Google websites, as I discussed in Sections VIII.D and VIII.E of my opening report.

58. Professor Zervas notes that "many websites make use of third-party services that provide features or functionality that the website owner desires but does not have the resources to develop themselves" and that such third-party services include Google Analytics and Google Ad Manager, among service providers such as Adobe, Stripe, PayPal, and others (¶ 39). But unlike these other service providers, Google is unique in its position as both a website service provider and a browser provider. It is a browser provider that provides users with a private browsing mode – Incognito – for which Google has made certain privacy representations to its users. In addition, Google makes use of private browsing mode data, not only to provide certain services, but also to enhance its own advertisement business and improve its other products and processes. Indeed, when Plaintiffs' counsel sought to take a Rule 30(b)(6) deposition concerning "Google's use of private browsing information, in whatever form, to improve Google's product and service offerings as well as its

business processes," Google objected on the ground that the testimony "would implicate dozens of Google business units and products," making it "overly broad." Dkt. 411-1 at 31.

59. Third, Professor Zervas ignores a key difference between Firefox private browsing modes and other private browsing modes. As I explained in my opening report (*see e.g.*, Section VIII.E.4 and Appendix D), Firefox implemented Enhanced Tracking Protection (ETP), which blocked cookies and/or restricted cookie usage several years before Chrome implemented [redacted]. In addition, Firefox implemented Tracking Protection by default for its private browsing mode in 2015, which blocked tracking beacons, including Google Analytics and ads tracking beacons. Google's response to these privacy measures was to implement a series of workarounds to mitigate its revenue loss as I explained in my opening report Section VIII.E.4.

60. Fourth, Professor Zervas fails to account for user misconceptions regarding private browsing functionality, which Google employees repeatedly referred to as "common" misconceptions among "most" private browsing mode users, across the different private browsing modes (*See* Opening Report Section VIII.J). Professor Zervas asserts that the private browsing modes "provide similar functionality" without addressing what Google employees referred to as "known" misconceptions regarding that functionality, especially regarding whether Google collects private browsing information. Google employees discussed how Google's own actions (including by using the Incognito brand with other products) was creating a "false sense of security" among users, with Google needing to "re-brand Incognito as something more honest and understandable" (GOOG-CABR-04971904). But Google did not make any such change to address misconceptions, instead continuing to represent to users that Google would not collect their private browsing information.

61. Fifth, one common misconception among Incognito users (according to Google's own employees) has been Google's "session-based tracking," whereby Google designed Chrome to share cookies across different Incognito windows and tabs (*See* Opening Report Se*ction* VIII.J.2). This is particularly problematic if a user signs into Google in one Incognito window. Google then tracks her subsequent browsing information on non-Google websites as "signed-in" GAIA data, even if such browsing took place in other Incognito windows. Other browsers, such as Safari, implemented separate cookie jars across different private browsing windows to prevent such tracking while Chrome did not. Safari launched its private browsing mode first, yet Google chose to design the Chrome private browsing mode (Incognito) to provide less privacy than Safari, with a different functionality. Google has the technical skills to produce a version of Chrome that meets or exceeds the capabilities of Apple's Safari browser, but Google chose to make an inferior product in terms of privacy properties.

C. Professor Zervas's opinions regarding the deletion of data are misleading because he fails to address how *Google* stored and used private browsing information irrespective of browsers discarding cookies or browsing history.

62. Professor Zervas discussed several tests he conducted to confirm certain browser functions when a private browsing "session" is closed (*see e.g.*, ¶ 5 and Section IV.C of his report). He concluded that "Private Browsing Modes [] prevent browsing history from being saved on the device." (¶ 5). This assertion is contrary to studies produced by Google in this case that have shown "private browsing mode does leave browsing evidence even after the browsers were closed", including browsing history (GOOG-CABR-04665148 at -152 and -154) and "Note e.g. https://www.quora.com/How-can-I-know-if-my-husband-uses-incognito-mode-on-Google, the `ipconfig /displaydns` command. That's not even malware" (GOOG-CABR-04696662 at -665.R).

63. Regardless, Professor Zervas's tests entirely missed the point. Plaintiffs' allegations and claims focus on Google's interception of private browsing communications, with Google

collecting, storing, and using private browsing information. Those allegations and claims focus on the storage and use on Google's servers, not on the browser.

64. As an example, consider a bugging device installed in a phone that transmits the audio to the spy next door. There would not need to be any recording stored on the phone, because it is separately being stored by the spy next door. There is no need to have two copies. Here, Professor Zervas is suggesting that the lack of a copy on the device (i.e., the user's computer) is the only relevant inquiry, but the fact is that Google has already used the device to intercept the private browsing communication and stored the information on Google's servers. At that point, there is no need for Google to have or keep any copy on the device itself.

D. Professor Zervas failed to consider other ways Google links data and tracks users.

65. Professor Zervas discusses in Sections V.A and V.B of his report certain Analytics settings and Ad Manager settings for web developers; however, notably there is not a single setting available for developers that is specific to private browsing mode. As I discussed in Section VIII.C of my opening report, the settings Google offers are all-or-nothing switches that impact both regular and private browsing. And again, all of the private and non-private browsing data is collected by the same Google services.

66. Professor Zervas discusses cookies extensively in his report but fails to address other ways Google tracks users with link decorations, signed-in identifiers on non-Google websites, IP address, and other fingerprinting information, which I discussed in my opening report (see e.g., Sections VIII.A and VIII.D and VIII.F) and above. [redacted] (GOOG-BRWN-00029326).

[redacted]

67. The same fingerprinting techniques can be used to identify class members, including for purposes of verifying a person's claim that he or she used Incognito. GOOG-CABR-04308776 at -777 lists a few fingerprinting parameters [redacted] These fingerprinting parameters are found in Google's analytics and ads logs. For example, on April 30, 2022, Google produced data in several ads logs.[36] As an example, [redacted] is associated with Plaintiff [redacted] Biscotti ID [redacted] in an Incognito browsing session.[37] Row 2 shows an exemplary event entry containing time stamp, IP address, user agent, DisplayLang ([redacted]"), [redacted] ("[redacted]"), HeaderOrder (indicating the order in which HTTP header information appear[38]), referer URL [redacted] redirect URL [redacted] and HTTPHeader. The HTTPHeader itself contains a myriad of information shown below, including "sec-ch-ua", "sec-ch-ua-platform", "accept", "accept-language", "Cookie" and "Accept-Encoding", among other fingerprinting information. Since this is from an Incognito session, the "X-Google-GFE-Original-X-Client-Data" field is empty. Additional fingerprinting information are contained in X-Google-GFE-Frontline-Info, including

[36] 2022-04-30 Brown v. Google - [redacted] Ads – AEO

[37] I explained in Appendix I of my opening report that Biscotti ID [redacted] belongs to Mr. Brown's Incognito session and the "maybe_chrome_incognito" bit in [redacted] display logs shows that the browsing session is Incognito.

[38] Different browsers send different header information and in different order. https://chris124567.github.io/2021-06-15-websites-lying-user-agent/ (Last accessed on May 30, 2022).

client country [redacted] Autonomous System Number (ASN)[39] and a pzf parameter[40] [redacted]

[redacted]

[redacted]

[redacted] (GOOG-CABR-04605197 at -199).

[39] https://www.iana.org/assignments/as-numbers/as-numbers.xhtml "Autonomous System (AS) Numbers are used by various routing protocols. IANA allocates AS Numbers to Regional Internet Registries (RIRs). The RIRs further allocate or assign AS Numbers to network operators in line with RIR policies." (Last accessed on May 30, 2022).

[40] https://lcamtuf.coredump.cx/p0f3/ "P0f is a tool that utilizes an array of sophisticated, purely passive traffic fingerprinting mechanisms to identify the players behind any incidental TCP/IP communications (often as little as a single normal SYN) without interfering in any way." (Last accessed on May 30, 2022).

68. In the table below, I include pzf, asn and cc values from the signed-out display ads data Google produced after April 30 associated with Biscotti IDs and IP addresses submitted as a part of the Third Iterative Search. As can be observed, these fingerprinting values can be used to distinguish between different users' browsers.

Contains Material Designated "Highly Confidential – Attorneys' Eyes Only" by Plaintiffs

Name	Biscotti ID	Browsing Mode	IP Address	Pzf	asn	cc
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]S
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Brown	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Byatt	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Castillo	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Castillo	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]S
Dai	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Dai	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]

Davis	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Davis	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Davis	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]S
Davis	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Davis	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Davis	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Davis	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]
Davis	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Trujillo	[redacted]	Regular	[redacted]	[redacted]	[redacted]	[redacted]
Trujillo	[redacted]	Incognito	[redacted]	[redacted]	[redacted]	[redacted]

69. In ¶ 98 of his report, Professor Zervas discusses IP address anonymization for Google Analytics. Since Professor Zervas's report does not evaluate actual stored data in Google's logs, he may believe that IP address anonymization provides a level of protection for the users. However, as I have observed in Plaintiff's Analytics data, IP addresses can be deanonymized based on other information stored in the logs. For example, from the Second Iterative Search in the Special Master Process, both the full IP address [redacted] and the "anonymized" version [redacted] are stored within the same log "[redacted]", produced on March 25, 2022. These two IP address versions are associated with the same Analytics UID [redacted] which identifies the same user. In addition, I have shown in Section VIII.F of my opening report that Analytics data can be linked to display ads data through various identifiers. Thus, other fingerprinting information can be used to deanonymize IP addresses in Google's logs.

70. Some features Professor Zervas discusses have not been available since the beginning of the class period. For example, Professor Zervas explains that "Consent Mode" became available in August 2020. Google Signals was fully launched in September 2018 (GOOG-BRWN-00711633 at -635). The [redacted] and [redacted] was launched in 2020 (GOOG-BRWN-00487443). "Limited Ads" was launched in 2021 (GOOG-CABR-04824758). Even when personalization of ads is disabled, Google still serves contextualized ads based on the user's location and the website visited, as Professor Zervas acknowledges (¶ 111).

71. In addition, some of the purported pro-privacy options Professor Zervas discusses, such as "Consent Mode", (¶ 96) are illusory as Google has already implemented workarounds. For example, GOOG-BRWN-00027028 [redacted]

[redacted]

[redacted]

[redacted]

E. Professor Zervas's "other settings and available features" are either unworkable or could have been implemented by Google.

72. Professor Zervas's examples of "other settings and available features that prevent the transmission of certain categories of At-Issue Data" (¶ 9) range from unworkable proposals to features that Google could easily implement into Chrome Incognito and/or its tracking beacons.

73. Fundamentally, Incognito mode itself is a promise of privacy. As Professor Zervas explained, Incognito "is not the default browsing mode" (¶ 49) – a user seeking a private browsing experience deliberately opens an Incognito window for private browsing. Google does not explain on the Incognito Splash Screen or on any webpage I have reviewed that a user must employ additional controls to stop Google's collection of private browsing information.

74. Instead, Google has ignored its own employees' pleas to inform users that Incognito does not prevent Google from collecting their browsing data. In Section VIII.K of my opening report, I discussed [redacted]

[redacted]

[redacted]

75. Professor Zervas opines that "browsers (including Chrome) have numerous *other* settings and available features that prevent the transmission of certain categories of At-Issue Data." ¶ 9. Some of the purported features he discusses do not provide workable solutions to user privacy, and instead show that Google prefers to maintain the status quo rather than make meaningful changes. Other controls and features that he discusses are things that Google could have easily implemented into Chrome Incognito and/or the Google tracking beacons at issue in this case. In other words, Google could have designed Chrome Incognito and its tracking beacons to provide what Professor Zervas's "other settings" provide. Still other features mentioned by Professor Zervas do not even prevent Google from collecting private browsing information from users' visits to non-Google websites. And for some purported controls, Google actually discourages users from employing them within an Incognito session.

76. Professor Zervas discusses the following settings:

(1) JavaScript Setting in Chrome

(2) Ad Blocking

(3) Google Analytics opt-out Browser add-on

(4) Cookie Setting in Chrome

(5) VPN

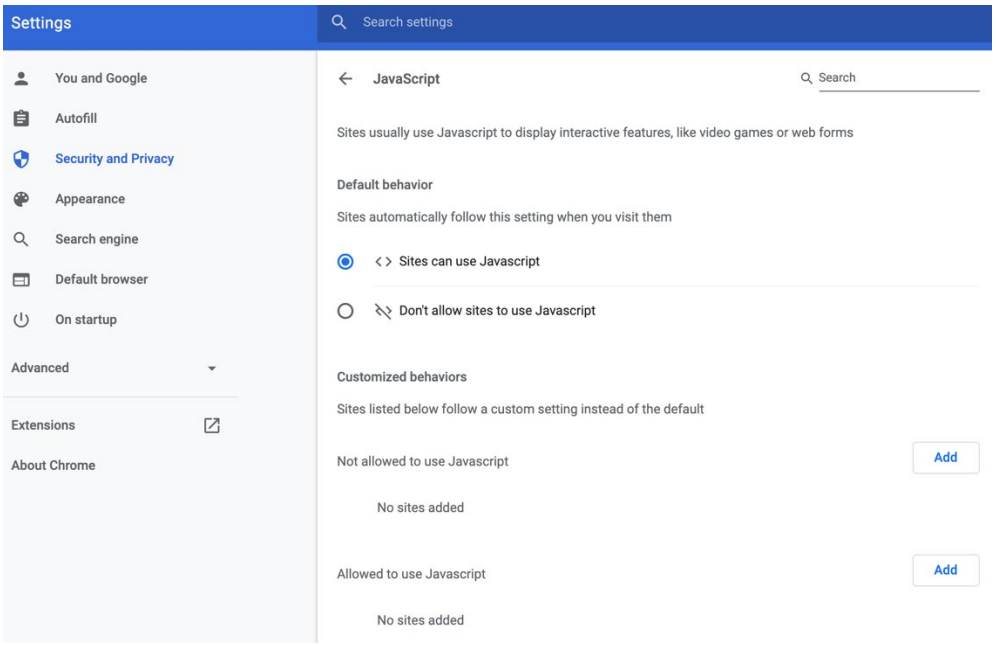
I discuss each below:

1. JavaScript Setting in Chrome

77. Professor Zervas states "Modern browsers contain built-in settings that disable JavaScript…Users also can install add-ons or extensions that would block JavaScript execution. To disable JavaScript using settings on Chrome, for example, users can enter *chrome://settings/content/javascript* in the address bar or navigate to the same page using setting pages" (¶ 103). Blocking JavaScript is not a default feature in Chrome Incognito mode, whereas Firefox Tracking Protection blocked Google Analytics and Ads tracking beacons by default in private browsing mode since 2015. Google could have incorporated default tracking beacon blocking in Incognito mode at least since the beginning of the class period, but Google did not.

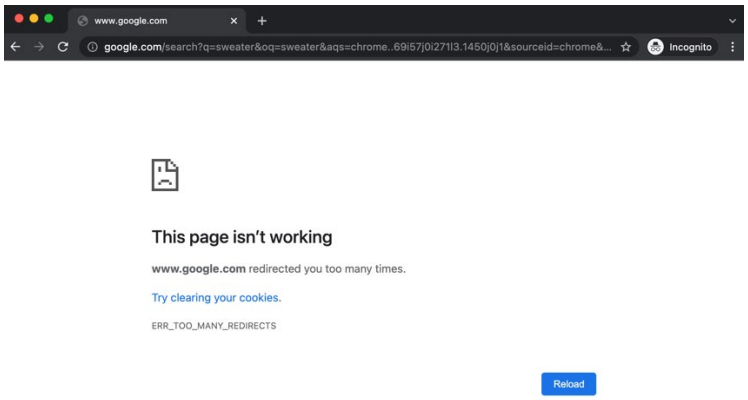
78. Unless a user is remarkably familiar with Chrome, they are not going to have the URL "*chrome://settings/content/javascript*" committed to memory. To access Chrome's JavaScript setting in the browser, a user needs to navigate through five levels in Chrome Settings:

Chrome -> Settings -> Security and Privacy -> Site Settings -> Javascript

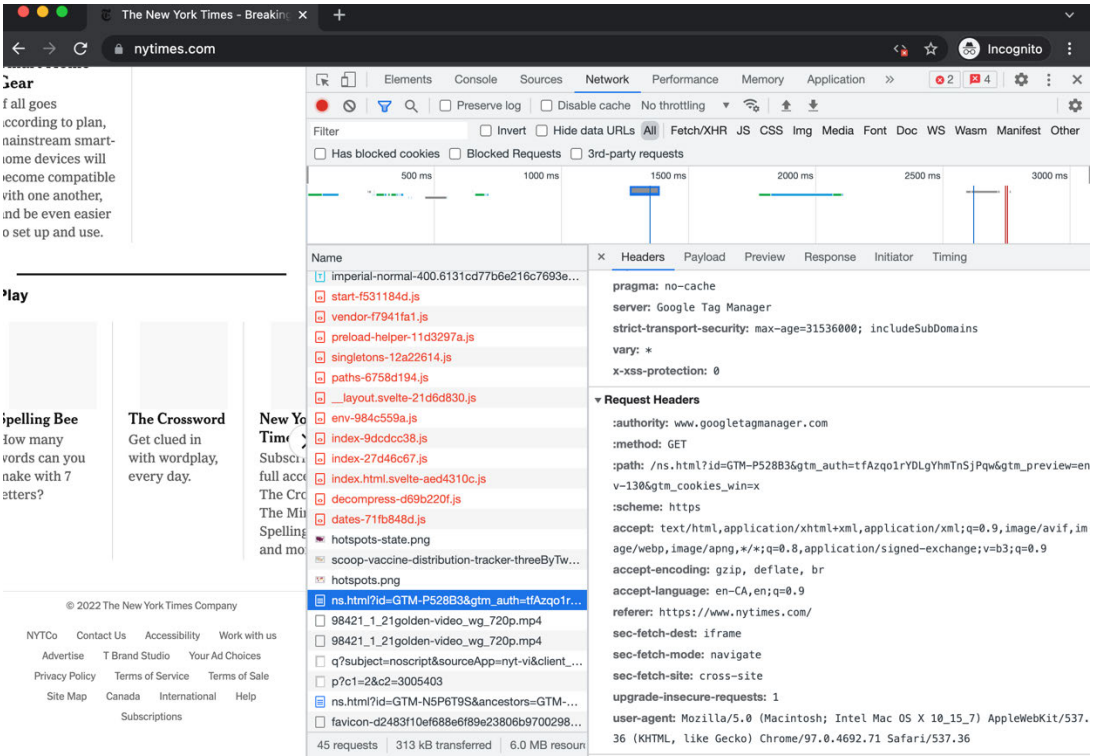


79. Note that on this setting page, Google says "Sites usually use Javascript to display interactive features, like video games or web forms." Google does not inform users that its JavaScript tracking beacons on third-party websites intercept users' private browsing communications with third-party websites and track users every step along the way while they browse non-Google websites in Incognito mode. Nor does Google provide users the option to only disable Google's JavaScript tracking beacons in Incognito mode.

80. Worse yet, when I selected the "Don't allow sites to use Javascript" option, started a brand new Incognito session and typed in a search term in Incognito's new tab page, I got the error message included below. Not only is Google's warning, "This page isn't working," a strong signal for a user to turn JavaScript back on, its advice, "Try clearing your cookies," makes little sense given Google's representation that a brand-new Incognito window starts with an empty cookie jar.



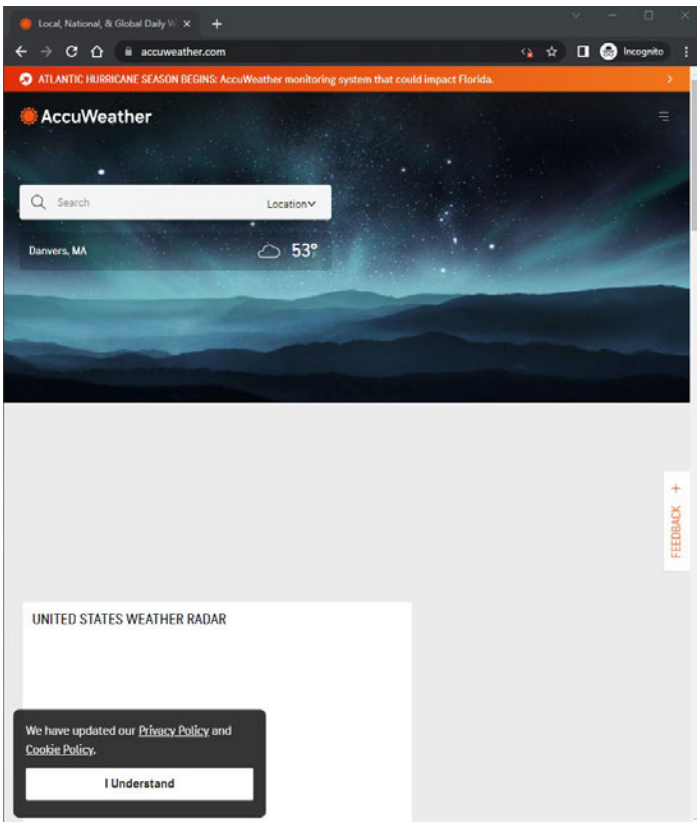
81. At this point, the only thing I could do in Incognito mode was to type in a complete URL in the URL bar (since omnibox search does not work). I went to https://www.nytimes.com/ and expected to not see any message being sent to Google. However, googletagmanager.com was still receiving my information, including the URL, user agent, and IP address along with other information. Thus, even with JavaScript disabled, Google was still intercepting and receiving my private browsing communications with New York Times.



82. This tracking occurs because Google instructs websites to install Google Tag Manager twice on every page: once in the <head> section of a page and once more in a <noscript> section[41]. This second tracking beacon in the <noscript> section intercepts communications and sends private communications to Google even if a user disables JavaScript in Chrome settings.

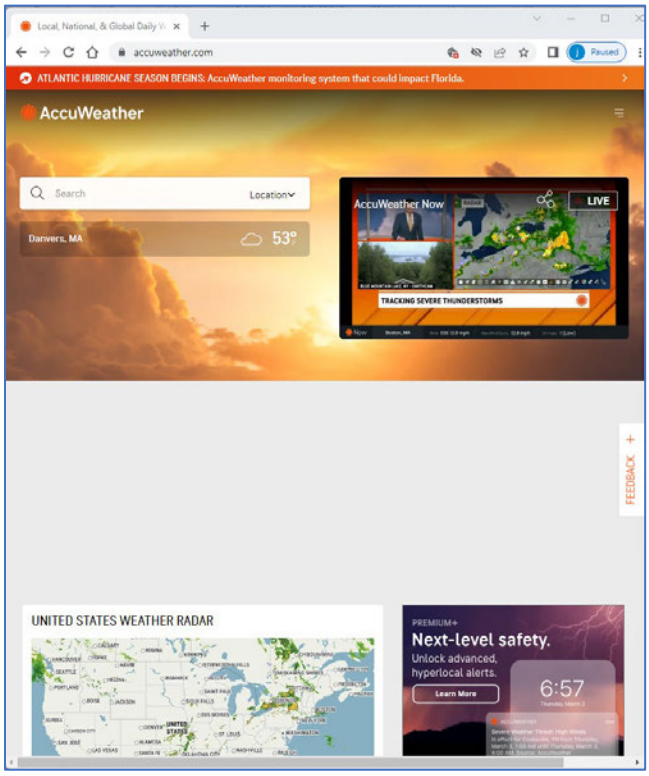
83. Moreover, a considerable number of popular websites require JavaScript be enabled to function correctly. Examples include:

a. **AccuWeather:** Google in its response to Interrogatory No. 5 identified the Accueather.com domain to have the highest website traffic in terms of (1) total Ad Manager Ad Requests and (2) visits from unique client IDs, each for a specific period. When the JavaScript execution is disabled for the Chrome browser, the www.accuweather.com webpage is unable to display any of the Google ads, any weather data maps, or video as illustrated by the images shown below.



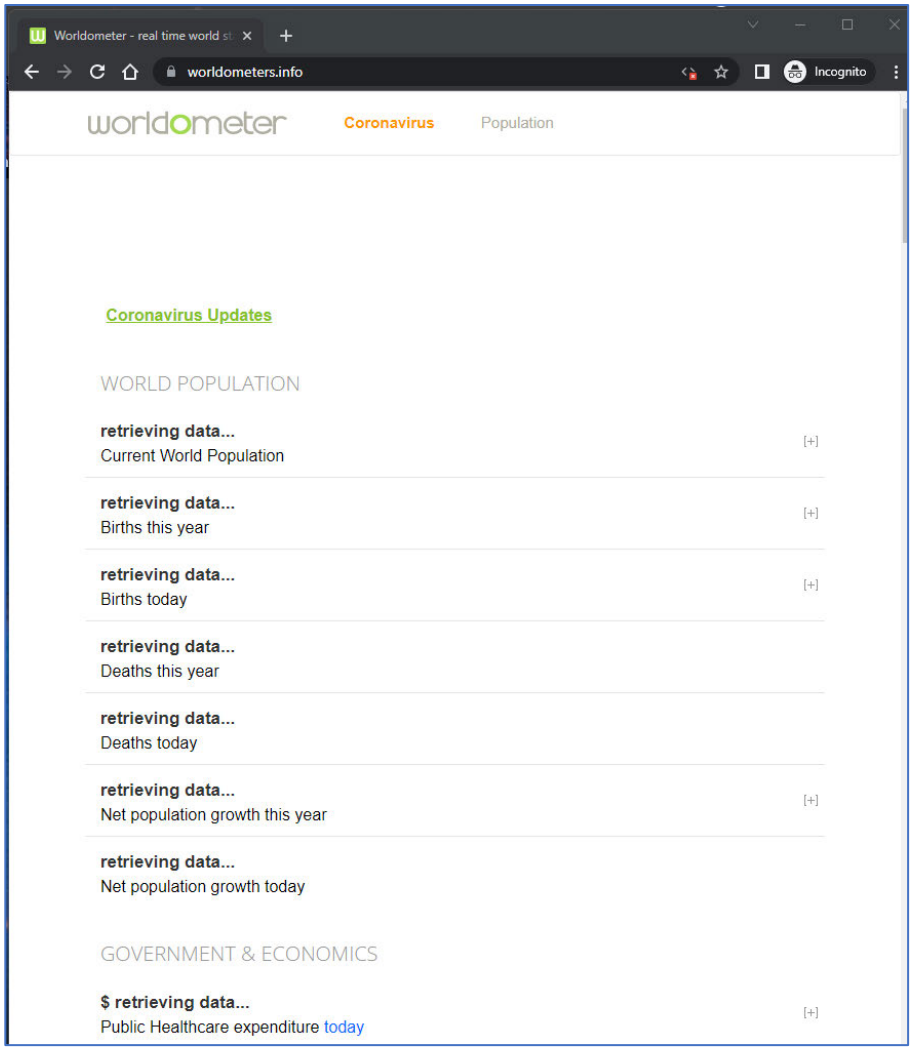
[41] https://developers.google.com/tag-platform/tag-manager/web (Last accessed on May 30, 2022).

www.accuweather.com homepage with the JavaScript execution disabled

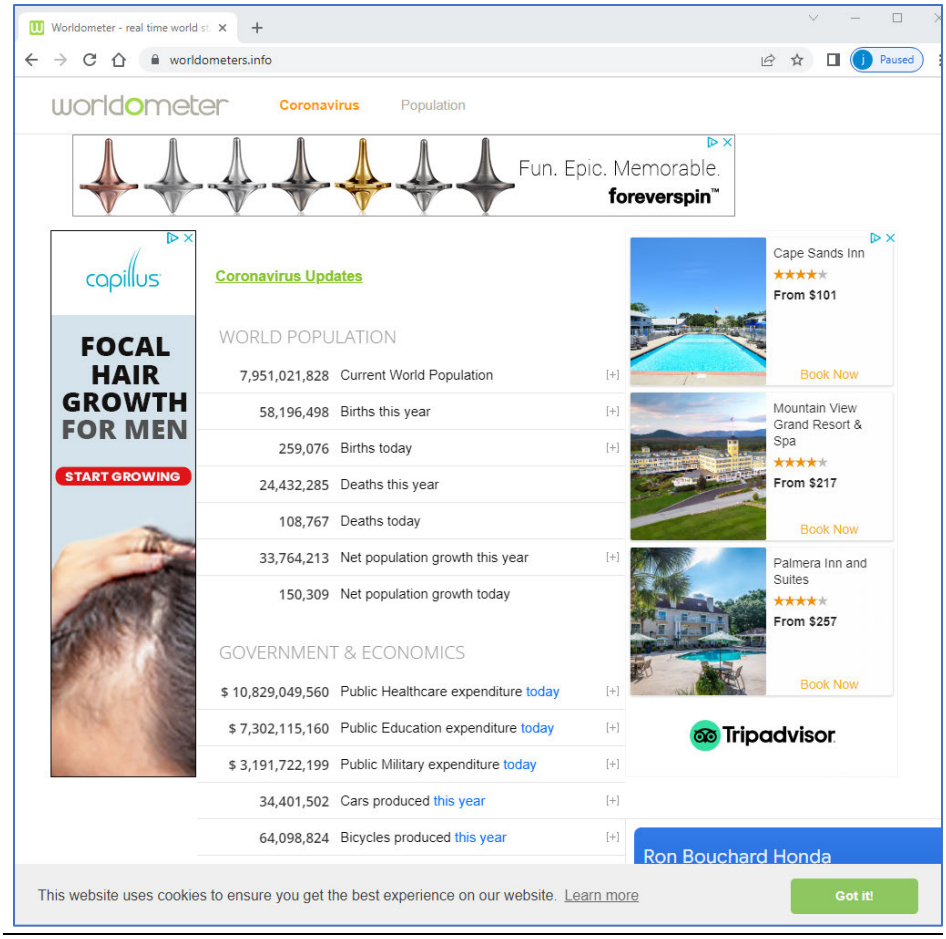


www.accuweather.com webpage with the JavaScript execution not disabled

b. **Worldometers**: Google also identified the Worldometers.info domain to have one of the highest website traffic figures in terms of total visits from unique client IDs for a specific period. When the JavaScript execution is disabled for the Chrome browser, the www.worldometers.info webpage was unable to display statistical data, information, or Google Ads as illustrated below.

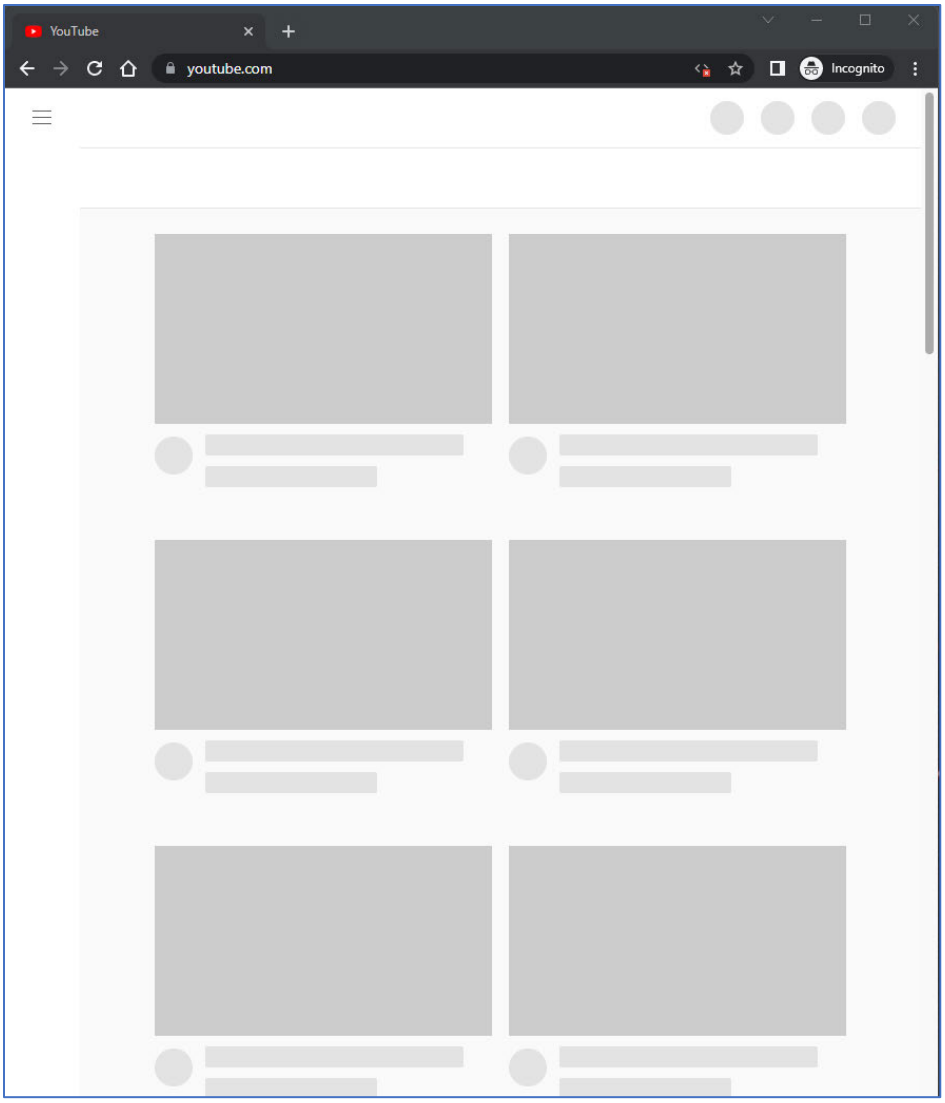


www.worldometers.info webpage with the JavaScript execution disabled

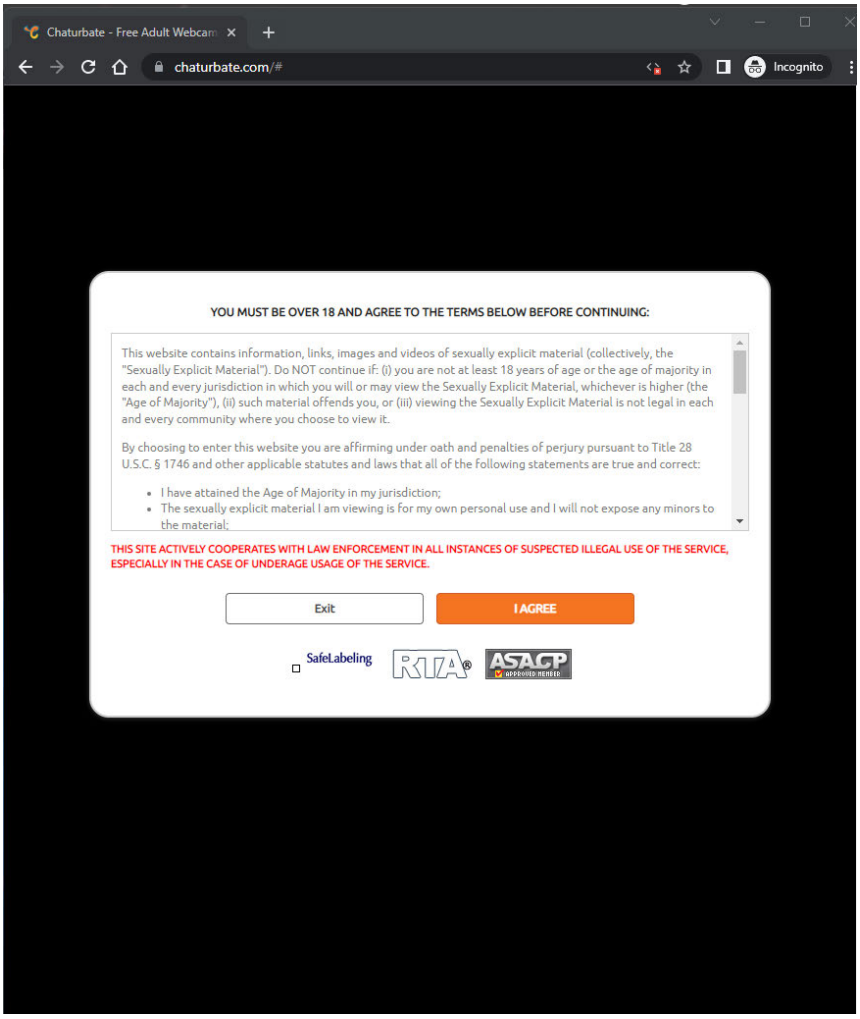


www.worldometers.info webpage with the JavaScript execution not disabled.

c. In addition, Google's owned and operated website, YouTube.com, which was identified by Google as a top Google advertisement traffic site, does not display any content when JavaScript is disabled—making the site completely unusable.



d. When a user has disabled the execution of JavaScript in the Chrome browser, he or she will be unable to provide the age confirmation on chaturbate.com webpage required to enter the site, rendering the website unusable. Google also identified this website as a top site for Google Analytics traffic.



84. My consultants conducted the same test for the 45 websites that Google identified in its response to Interrogatory No. 5 (the websites containing the highest traffic in terms of total visits from unique client IDs for Google Ad Manager or Google Analytics). When the JavaScript execution is disabled for the Chrome, 19 of these websites were not usable, and 18 websites had diminished capabilities. (*See* Exhibit C).

85. Many of the above experiments were repeated to view the same webpages using all versions of the Chrome browser from 2016 until today, and comparable results were observed (*See* Appendix I-2).

86. Professor Zervas also notes that "Users also can install add-ons or extensions that would block JavaScript execution." (¶ 103), and he references the Sybu JavaScript Blocker add-on. My consultants conducted the same tests described above, this time with the Sybu Javascript Blocker extension enabled for Incognito mode, and the results were identical. A considerable number of the websites were unusable. *See* Appendix I-3 and Appendix I-4 for additional details.

87. Professor Zervas relies on a 2015 document to suggest that disabling JavaScript "depending on the user's browsing behavior, it may not lead to reduced functionality for many websites." (¶ 104). However, since 2015, publishers' reliance on JavaScript has increased, and the above examples show that JavaScript is essential for most webpages.

88. For the above reasons, it is impractical to require privacy-seeking users to disable JavaScript. Nor is it necessary. For example, Firefox's Tracking Protection and Enhanced Tracking Protection blocked only Analytics and ads tracking beacons and other harmful trackers, without blocking other JavaScript necessary for normal website functions.[42] Professor Zervas does not explain why Google would not do the same.

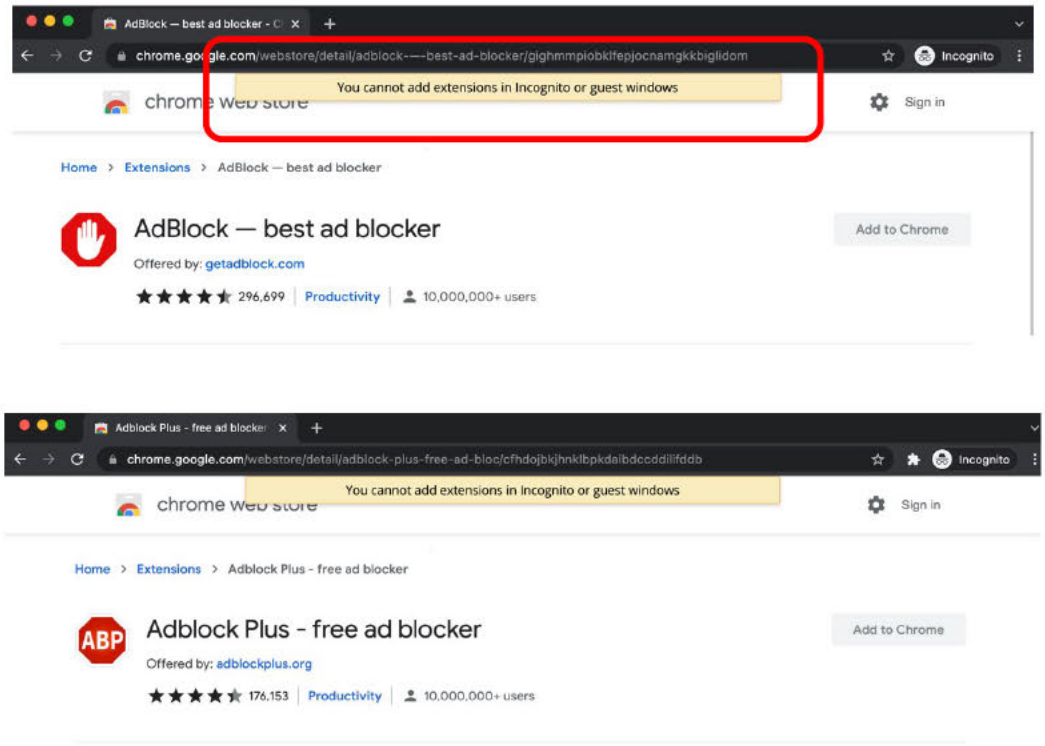
2. Ad Blocking

89. Professor Zervas states that "Chrome users can also install extensions that may alter the flow of data to Google Ad Manager, such as Ad Blocker extensions. For example, Chrome users can install the uBlock or AdBlock extensions" (¶ 114).

90. Google does not explain in Chrome settings or Google account settings how users can or should use ad blocking extensions to block Google's ad tracking beacons. To the contrary, Google's messaging deters users from trying to use such features within Incognito.

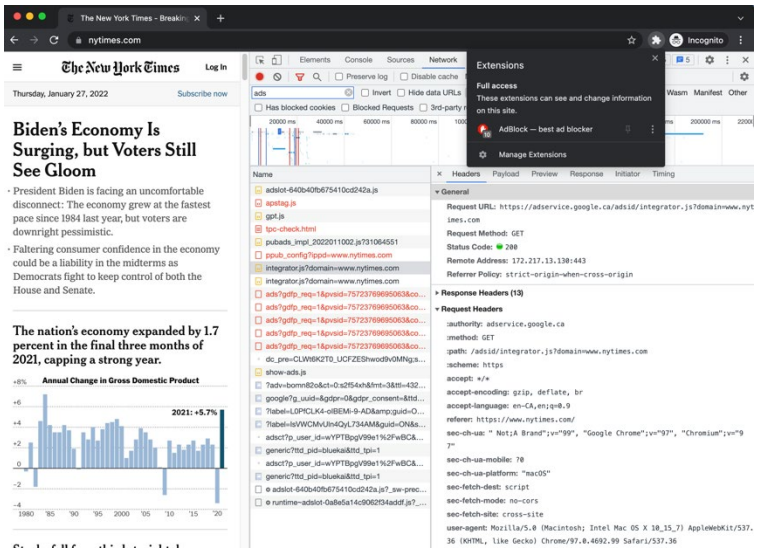
[42] https://support mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop (Last accessed on May 30, 2022).

91. When users do try to install any ad blocking extension in Incognito mode, they will see a message informing them that "You cannot add extensions in Incognito or guest windows", as indicated in the screen capture below.



92. If the user tries to install the ad blocking extension in non-Incognito mode, it will be disabled by default in Incognito mode while enabled by default in non-Incognito mode. Note that in one of Google's help pages, Google explains to users that "If you see a message saying 'Extensions Disabled,' it's because Chrome has turned off one or more of your extensions to keep your data safe while you're browsing the Internet. The extensions that Chrome turned off either didn't come from the Chrome Web Store or were determined unsafe." Since AdBlock and Adblock Plus are both extensions available from the Chrome Web Store, Google's explanation may lead users to believe that these ad blocking extensions are "unsafe" and that users are better off ("to keep your data safe") without them.

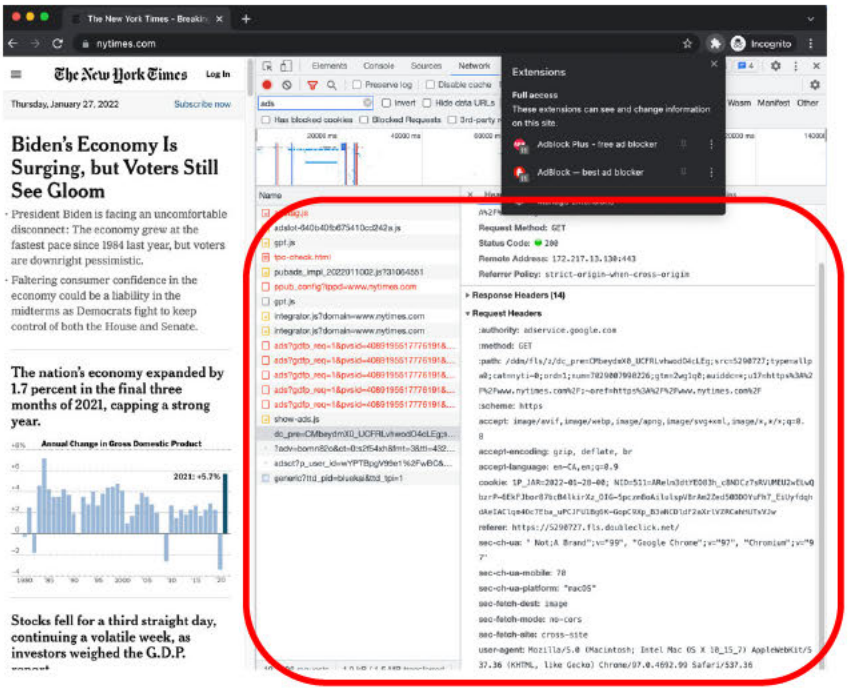
93. In any event, these extensions *still* do not prevent Google from intercepting the user's private browsing communications. For example, when I went to https://www.nytimes.com/ in Incognito mode with AdBlock enabled, a message was sent to Google along with user-agent, referrer, and IP address.



94. I installed and enabled Adblock Plus as well. Even with both ad blocker extensions enabled in Incognito mode, Google was still intercepting those communications to collect information from the private browsing.

URL:

https://[redacted]/ddm/fls/z/dc_pre=CMbeydmX0_UCFRLvhwodO4cLEg;src=5290727;type=allpa0;cat=nyti-0;ord=1;num=7029007990226;gtm=2wg1q0;auiddc=*;u17=https://www.nytimes.com/;~oref=[redacted]



95. Professor Zervas also states that "users can choose to install a dedicated standalone application that would block ads, such as AdGuard" (¶ 114). Again, ad blocking software does not block all Google tracking, as explained above.

96. Additionally, Professor Zervas asserts that "Users can also install the Interest-Based Advertising (IBA) Opt-out extension provided by Google which allows opting out of personalized ads. This extension allows users to opt out of DoubleClick advertising cookies, which are used by Google to display personalized ads" (¶ 114). Professor Zervas refers to "IBA Opt-out (by Google)," Chrome Web Store, Google, available at https://chrome.google.com/webstore/detail/iba-opt-out-by-google/gbiekjoijknlhijdjbaadobpkdhmoebb?hl=en as the URL to download. But as explained before, the Chrome extension is not enabled for Incognito mode by default.

97. And even if the user enables the extension for Incognito mode, Google advertisements are still displayed. Accordingly, Google tracking beacons are still functioning, and at least some of

the user's private browsing information, such as IP address, user agent string, and URL of the web page viewed, is collected by Google and sent to Google's servers (*See* Appendix I-3).

98. Professor Zervas also states "In addition, users can also opt out of personalized ads on the NAI Consumer Opt Out page. This service allows users to 'choose to opt out of Interest-Based Advertising from one, some or all participating NAI member companies on your browser.'" For this proposition, Professor Zervas references footnote 147, which includes the https://thenai.org/opt-out/" URL. (¶ 114). We visited the referenced webpage and selected to opt-out of all identified websites. Subsequently, when a webpage that displays Google-supplied advertisements is visited, the webpage still displayed the Google supplied advertisements. Accordingly, Google tracking beacons are still downloaded, and at least some of the user's private browsing information is collected by Google and sent to Google's servers. (*See* Appendix I-5)

99. Professor Zervas also states that "Users can also affect personalized advertising functionalities by visiting *https://adssettings.google.com/*.... where they can choose what types of ads they would like to see or turn off ad personalization." (¶ 115). However, Professor Zervas does not explain if and how changing personalization settings stops Google from collecting private browsing information. If Professor Zervas meant that turning off ad personalization stops Google from receiving user's private browsing information, he is incorrect. When a private browsing user turns off ad personalization while visiting a website that contains Google-provided advertisements, Google tracking beacons are still functioning, and at least some of the user's private browsing information, such as IP address, user agent string, and URL of the web page viewed, is collected by Google and sent to Google's servers. (*See* Appendix I-5)

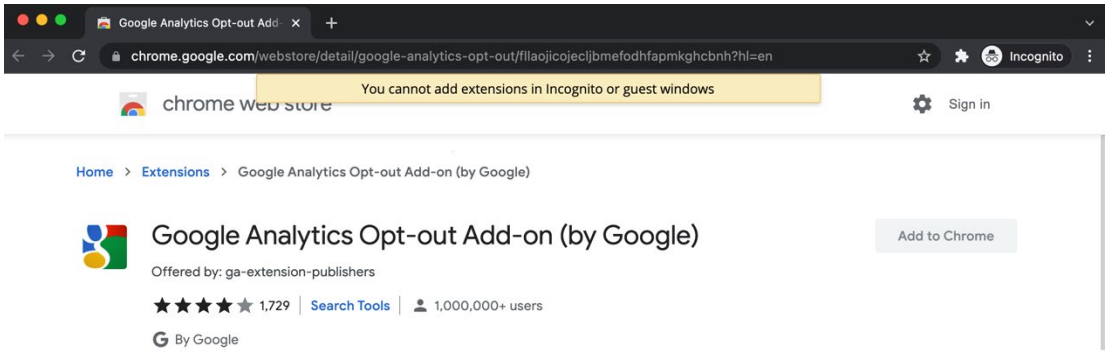
100. Further, Google does not explain in Chrome settings or Google Account settings how to use such ad blocker programs to block Google's advertising tracking beacons or even which ad

blocker program is safe to download and install. And the fact that Google claims that Google gives users privacy control but then points to third-party software to provide that privacy is the essence of chutzpah.

101. Finally, as far as Google believes that ad blocking extensions will provide users with privacy, then Google could have designed Chrome Incognito to include such functionality.

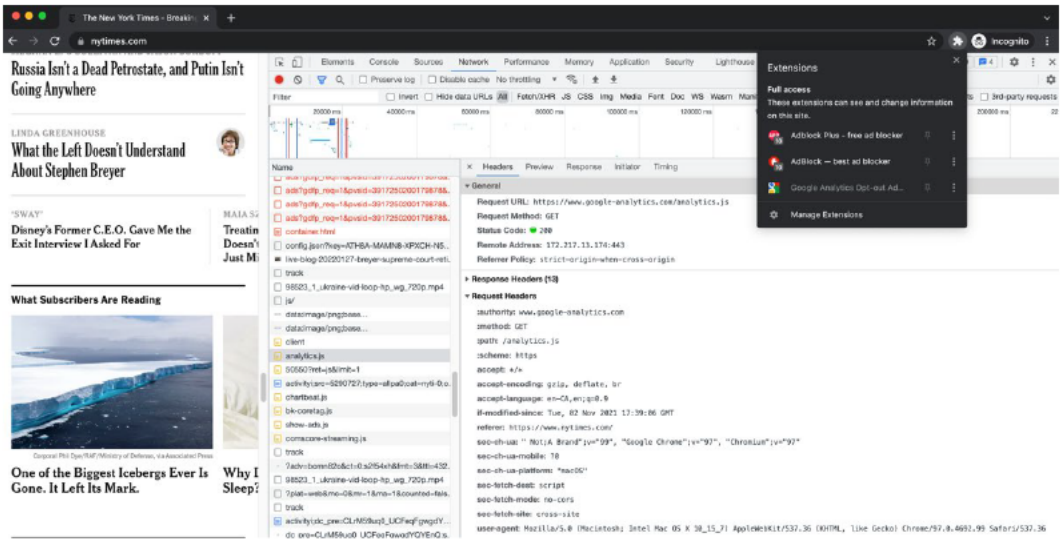
3. Google Analytics Opt-out Browser add on

102. Professor Zervas states that "Users can also install an extension called the 'Google Analytics Opt-out Browser Add-on'…this extension prevents the Google Analytics JavaScript code from transmitting information to Google Analytics" (¶ 102). As with other browser extensions, when users try to install this browser add-on in Incognito mode, they will see a message informing them that "You cannot add extensions in Incognito or guest windows" as indicated in the screen capture below. And, in any event, this browser add-on does not block all Google tracking as I show through testing in Appendix I-3.



103. Like other browser extensions, even if users figure out that this browser add-on can be installed in non-Incognito mode, it is disabled by default in Incognito mode. Ironically, this means that a user with ad blocking extensions and the Google Analytics Opt-out Add-on have less protection in Incognito mode than in non-Incognito mode. Furthermore, installing the Google Analytics Opt-out Add-on and allowing it for Incognito mode does not prevent Google from

intercepting the user's private browsing communications. For example, when I visited https://www.nytimes.com/ in Incognito mode with Google Analytics Opt-out Add-on enabled along with the two ad blocker extensions installed earlier, an analytics.js call still functions, intercepting the communication and sending private browsing information to Google along with user-agent, referrer, and IP address.



104. [redacted][43].

105. [redacted] But even if information copied and sent to Google do not contain visitor identifiers, they still contain identifying information such as a user's IP address and user-agent. [redacted]

[43] GOOG-CALH-00289665, see e.g., tabs: 2019-07-22 (All), 2018-04-06 (All), and 2017-03-24 (All).
[44] GOOG-CABR-00895413 at -414 and -415: [redacted]

[redacted] (GOOG-CABR-00895413 at -415).

106. Finally, as far as Google believes that this extension will provide users with privacy, then Google could have designed Chrome Incognito to include such a functionality.

4. Cookie Settings in Chrome

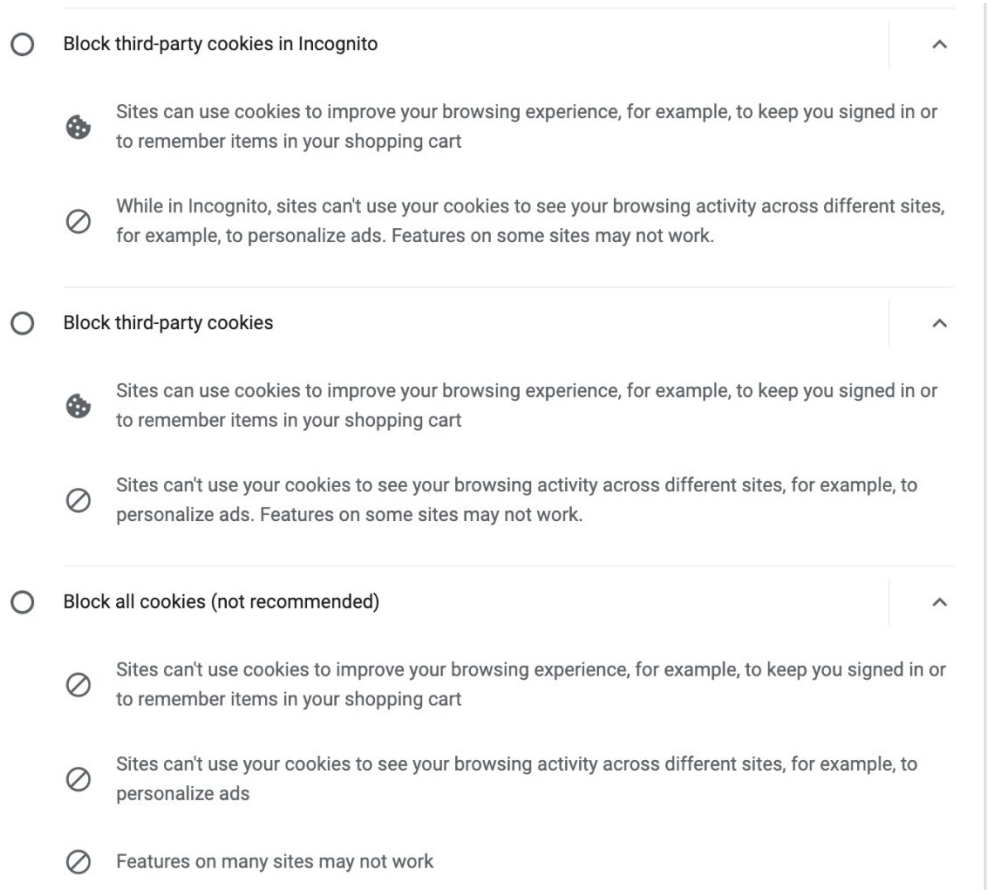
107. Professor Zervas states that "users can prevent transmission of cookies to Google Analytics by using browser cookie settings. In Chrome, these settings can be accessed by typing *chrome://settings/cookies* to the address bar or by accessing settings through navigation panes on the browser" (¶ 99). As far as Google believes that blocking all cookies is better for privacy, Google could have blocked all cookies by default within Incognito mode since the beginning of the class period.

108. Moreover, through tests, I show in Appendix I-1 that blocking cookies, even all cookies, does not block Google's interception of private browsing communications. Google also makes it difficult to find this option and then discourages users from using it. And enabling it makes a significant proportion of websites unusable.

109. Again, unless a user is remarkably familiar with Chrome, they will be unlikely to have the URL "*chrome://settings/cookies*" committed to memory. Access to the cookie settings in Chrome requires navigation through four levels of settings: Chrome -> Settings -> Security and Privacy -> Cookies and other site data. As Google's internal document acknowledges, "Chrome has existing

privacy features that allows blocking third-party cookies manually. However, these controls are too hard to find and understand" (GOOG-BRWN-00049022 at -024).

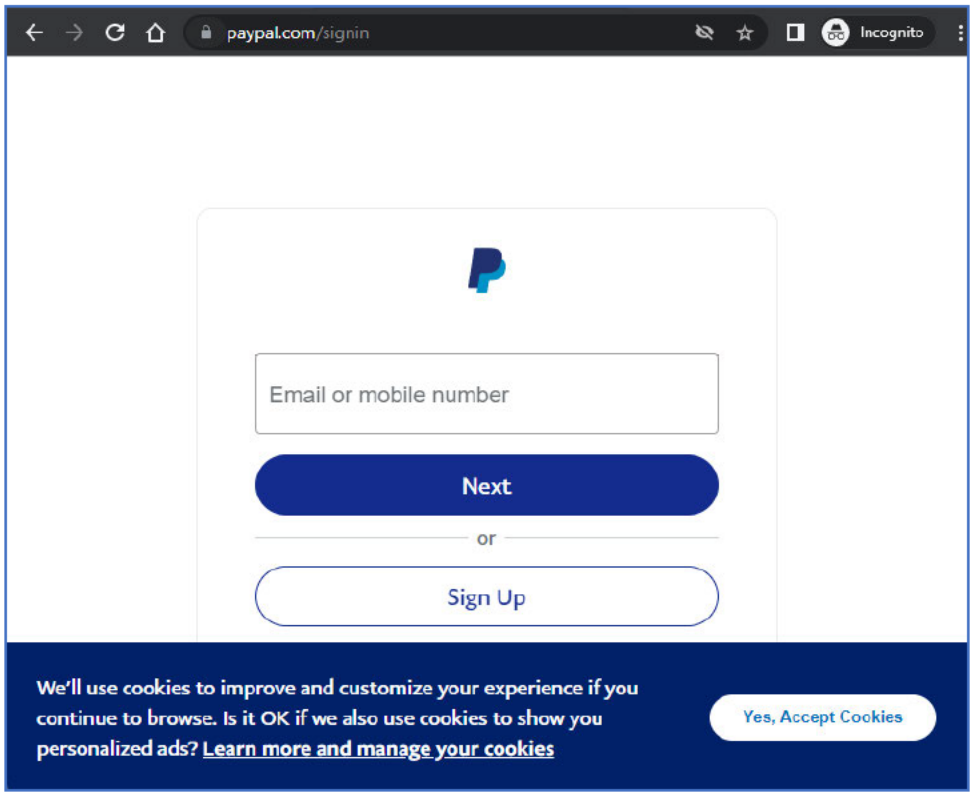
110. Within Chrome's cookie settings, the options for cookie blocking are "Block third-party cookies in Incognito", "Block third-party cookies", and "Block all cookies (not recommended)" as shown below. Notably, Google does not offer an option to block all cookies specifically in Incognito mode. If a user chooses "Block all cookies", which Google does not recommend, then cookies in both Incognito and non-Incognito mode are blocked. This blocking does not prevent Google tracking beacons from operating; it merely prevents Google from saving identifiers or other data in cookies on the user's computer. The user's private browsing activity, IP address, and user agent string, among other sensitive data, may still be collected by Google. [*See*, Appendix I-1]



111. The option to block third-party cookies in Incognito was referred to internally by Google as [redacted] This feature was first launched in May 2020 and was rolled out gradually over the course of 2020 on desktop and Android devices[45]. Thus, the [redacted] functionality was not in place for most of the class period, and it was never rolled out on iOS devices[46].

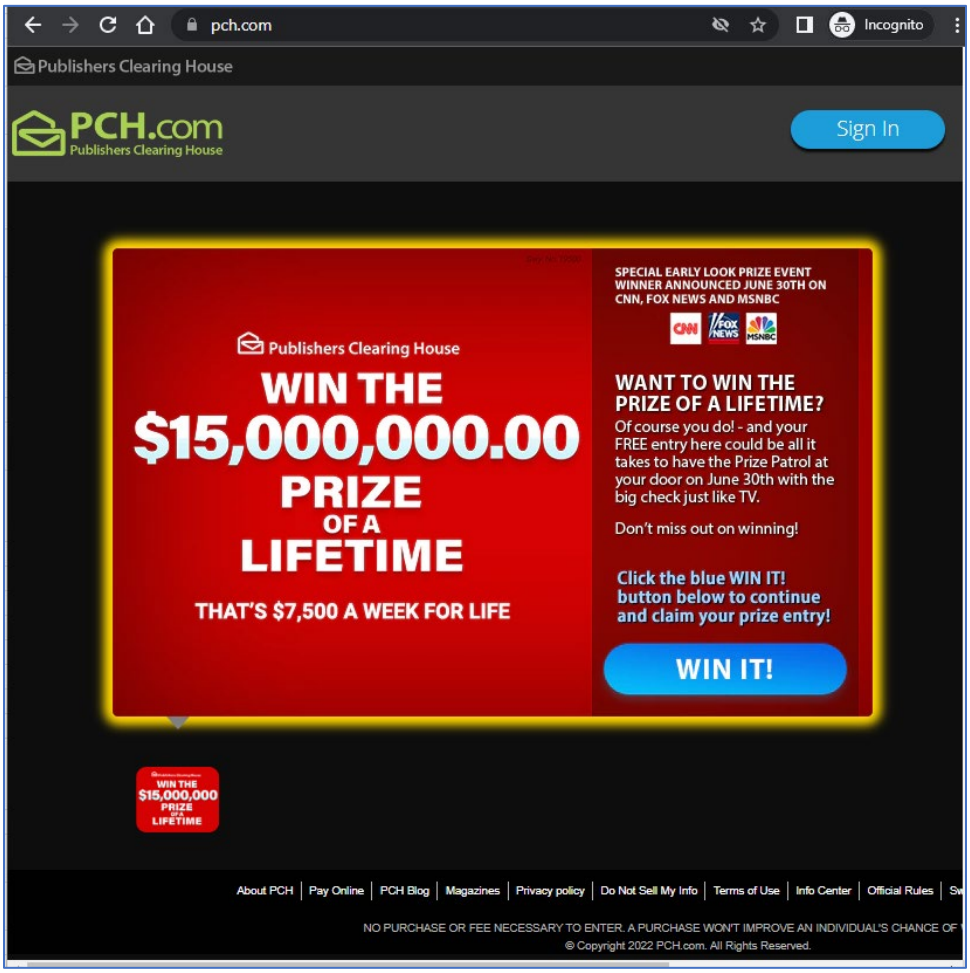
112. If despite Google's warning to the user not to block all cookies, should a user choose to block all cookies while browsing in Incognito mode, a considerable proportion of websites are not usable or are diminished in functionality.

113. For example, when a user visits paypal.com with all the cookies disabled, the user is not able to login to make or receive payments.



[45] GOOG-BRWN-00181499 at -499 and -500 discussing on July 13, 2020, plans to scale [redacted] on Desktop and Android and discussing on June 22, 2020, plans to scale [redacted] on Desktop and Android.
[46] GOOG-CABR-04986312

114. Similarly, when a user visits the pch.com website with all cookies disabled, most of the home page content and navigation drop down menus are not displayed:



115. My consultants ran tests to evaluate the effect on selecting 'Block all cookies" on the 45 top-level domain websites that Google identified in its response to Interrogatory No. 5 as the most trafficked websites in terms total visits from unique client IDs for Google Ad Manager or Google Analytics. 13 websites were not usable for the intended purposes and 10 websites had diminished capabilities. (*See* Exhibit C.) All of this suggests that users are unlikely to use this as an option, presuming they even know about this option at all.

116. If all cookies are blocked by the user, Google still receives private browsing information from its Google tracking beacons when a user views a webpage that has Google Analytics and/or Google Ads support. More specifically, even if a user blocks all cookies using the Chrome setting and then visits a webpage such as accuweather.com, the Google tracking beacons included in the webpage still transmit the user's private browsing information to Google servers (*See* Appendix I-1).

5. VPN

117. Professor Zervas states that "Users can also mask their IP address from Google Analytics and any other Internet services by using a VPN in both Regular and Private Browsing Modes" and cites a reference stating that "[redacted] of US and UK users use VPN services at least once a week" (¶ 105). This reference does not discuss what percentage of US users have used VPN services during the class period or in conjunction with private browsing, nor the percentage of private browsing traffic that is currently or at any point during the class period was served by VPN.

118. Professor Zervas also does not contend that use of a VPN would prevent Google from collecting other identifying information such as cookies and signed-in identifiers on non-Google websites, websites visited, and timestamps.

119. In addition, the fact that Professor Zervas identifies IP masking to be important for protecting privacy is telling. While he presents VPN as a way for users to protect their privacy, Professor Zervas did not in his report evaluate the implication of Google still collecting users' IP addresses from user's private browsing communications with non-Google websites. I would have expected Professor Zervas to evaluate Google's collection of IP address information before opining on whether private browsing information can be linked to users or devices, particularly since Professor Zervas appears to recognize the importance of masking IP address information.

120. In addition, as I explained in my opening report, Google could have redesigned Chrome Incognito [redacted] (GOOG-BRWN-00615433 at -434). But Google chose not to make those changes to Incognito mode. Professor Zervas ignores the implications of Google's choice.

* * *

121. Professor Zervas also offers no opinion or information about the number of users who employed any of the foregoing settings or features while in a private browsing mode. As far as private browsing users did employ such settings or features, and insofar as those settings or features impacted Google's collection of their private browsing information—as Professor Zervas suggests that it would—then Google's records would reflect that impact. Put differently, had Google preserved all private browsing data that it collected, then Google could verify whether it collected private browsing information from any individual who used Professor Zervas's settings and features. Moreover, as explained above in this section, to the extent any setting is not enabled by default on a browser, users must actively enable these settings and features, and the process of doing so is far more involved than merely opening a private browsing window. In any claims process, users could disclose whether they used any of these settings or features even while in a private browsing mode. Finally, Professor Zervas tellingly does not opine that these settings and features can be employed in such a way to entirely prevent Google's collection of private browsing data.

F. Professor Zervas wrongly opines that private browsing modes work as described in public documentation.

122. Professor Zervas asserts that "the Private Browsing modes work as described in public documentation" (Zervas Report ¶ 5). I disagree. As I explained in my opening report, "Google's Chrome Incognito mode functioned in ways that differed from how Google represented it would function," including within the Incognito Splash Screen, the Google Privacy Policy, Chrome Privacy Notice, and Search & browse Privately webpage. (Opening Report ¶ 318; *see also, e.g.*, *id.* ¶¶ 41-45.)

123. Professor Zervas's opinion also disregards and is inconsistent with statements made by many Google employees. My opening report cites numerous internal Google documents where Google employees recognized that users have "common misconceptions about private mode," including that it "hides browsing activity from Google" (GOOG-BRWN-00051239 at -267); *see also, e.g.*, Opening Report ¶¶ 322-34 (citing additional documents). Professor Zervas fails to address any of these internal Google documents.

124. Other internal Google documents support my opinion and undermine Professor Zervas's opinion. For example, in September 2014, a Google employee described a statement by Eric Schmidt, Google's Executive Chairman, as "clear evidence that people don't and indeed cannot understand Incognito's guarantee(s) and non-guarantee(s). Even Eric Schmidt . . . . Normal people have no chance" (GOOG-CABR-05477364 at -66). [redacted]

[redacted]

125. I also understand that Google in this case has taken the position that users consent to Google's collection of private browsing information as far as, according to Google, "[n]umerous third-party articles have explained that Google receives the at-issue data while users are in Incognito mode" (Google's Supp'l Response to Interrogatory 40).

126. As I understand it, Google has not made any assertions concerning whether or how many people accessed or read these articles. Assuming these websites were using Google Analytics or Google Ads at the time the article was released, Google at least at one point possessed statistics regarding how many users, if any, clicked on most of these articles (*see, e.g.*, GOOG-BRWN-00490767 at -772 (noting that Analytics tracking beacons are installed on more than [redacted] websites).

127. The articles Google cited in its Supplemental Response to Interrogatory No. 40 come from various non-Google websites. I understand from Counsel that Google refused to provide a list of all websites that use Google Analytics and Google Ad Manager. The Court then ruled that "before Google can argue or assert that any specific website did not use Google Analytics, Google must respond to this interrogatory as to that website at least 30 days in advance of making any such assertion or argument" (Dkt. 288-1 at 1). I also understand that the Court issued the same ruling as to Google Ad Manager (Dkt. 288-1 at 2). Google never provided such an update as to Google Analytics or Google Ad Manager, and discovery is now closed. I understand that Google is therefore precluded from arguing that any of the websites cited in Interrogatory No. 40 do not

contain Google tracking beacons. The implication is that Google has data on which and how many users clicked those articles and Google either (a) chose not to produce it and/or (b) already deleted it.

VI. CONCLUSION & RIGHT TO SUPPLEMENT

My investigation is ongoing. I reserve the right to update or supplement this report in reliance upon whatever further information becomes available.

Respectfully submitted by,

/s/ Jonathan E. Hochman
JE Hochman & Associates LLC
Date: June 7, 2022

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX A

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX B

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX C

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX D

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX E

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX F

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX G

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX H

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX I

Produced Electronically

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX J

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

APPENDIX K

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

EXHIBIT A

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

EXHIBIT B

Sealed Entirely

REBUTTAL REPORT OF JONATHAN E. HOCHMAN

JUNE 7, 2022

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, WILLIAM BYATT, JEREMY DAVIS, CHRISTOPHER CASTILLO, and MONIQUE TRUJILLO, individually and on behalf of all similarly situated,	§	
Plaintiffs,	§	**Case No. 4:20-cv-03664-YGR-SVK**
v.	§	
GOOGLE LLC,	§	
Defendant.	§	

EXHIBIT C

REBUTTAL TO REPORT OF GEORGIOS ZERVAS AND SUPPLEMENTAL REPORT OF JONATHAN E. HOCHMAN

June 7, 2022

Summary of Findings

When Javascript is disabled, of the 45 unique top-level domains websites identified by Google in its Interrogatory 5 Response:

19 websites are not usable for its intended use
18 websites have its capabilities diminished for its intended use

When All cookies are blocked, of the 45 unique top-level domains websites identified by Google in its Interrogatory 5 Response:

13 websites are not usable for its intended use
10 websites have its capabilities diminished for its intended use

Website	When Javascript is disabled	When all cookies are disabled
accuweather.com	Unusable	Unusable
apple.com	No impact	No impact
britannica.com	Limited impact	Limited impact
businessnsider.com	Diminished capabilities	Diminished capabilities
buzzfeed.com	Limited impact	Limited impact
cbslocal.com	Diminished capabilities	Diminished capabilities
change.org	Unusable	Unusable
chaturbate.com	Unusable	Unusable
chess.com	Unusable	No impact
cnn.com	Diminished capabilities	Diminished capabilities
condenast.com	No Impact	No impact
dailymail.co.uk	Diminished capabilities	Diminished capabilities
ebay.com	No impact	Limited impact
fandom.com	Limited impact	Limited impact
foxnews.com	Diminished capabilities	Diminished capabilities
grammarly.com	Diminished capabilities	Unusable
hearst.com	No Impact	No impact

Website	When Javascript is disabled	When all cookies are disabled
indeed.com	No impact	No impact
kohls.com	Unusable	Limited impact
linkedin.com	Unusable	Unusable
nexstar.tv	Diminished capabilities	No impact
nypost.com	Diminished capabilities	Limited impact
nytimes.com	Diminished capabilities	Diminished capabilities
paypal.com	Unusable	Unusable
pch.com	Unusable	Diminished capabilities
pornhub.com	Unusable	No impact
privy.com	Unusable	No impact
quizlet.com	Unusable	Unusable
realtor.com	Unusable	No impact
reddit.com	Unusable	Unusable
roblox.com	Unusable	Unusable
surveymonkey.com	Unusable	No impact
target.com	Unusable	Unusable
townnews.com	Diminished capabilities	No impact

Website	When Javascript is disabled	When all cookies are disabled
usatoday.com	Diminished capabilities	Diminished capabilities
vdo.ai	Diminished capabilities	Unusable
Vogue.com (CondeNast site)	Diminished capabilities	Unusable
washingtonpost.com	Diminished capabilities	Unusable
weather.com	Diminished capabilities	Diminished capabilities
webmd.com	Diminished capabilities	Diminished capabilities
wikia.com	Diminished capabilities	No impact
worldometers.info	Unusable	No impact
youtube.com	Unusable	No impact
yummly.com	Unusable	No impact
zynga.com	Diminished capabilities	No impact